UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation This Document Relates to: All Consumer Cases	MDL No. 14-2522 (PAM/JJK) **CONSUMER PLAINTIFFS' FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

TABLE OF CONTENTS

Plaintiffs identified below (collectively, "Consumer Plaintiffs"), individually and on behalf of the Classes defined below of similarly situated persons, file this First Amended Consolidated Class Action Complaint pursuant to Rule 15(a)(2) of the Federal Rules of Civil Procedure based on the written consent of Defendant and pursuant to the Court's Pretrial Scheduling Order (ECF No. 94). Consumer Plaintiffs allege the following claims against Target Corporation ("Target" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

I. SUMMARY OF ACTION

1. Between approximately November 15, 2013 and December 17, 2013, Target was subject to one of the largest data breaches in history ("the Target data breach"), when hackers stole the personal and financial information of up to 110 million Target customers. Target's conduct – failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' financial account and personal data, and failing to provide timely and adequate notice of the Target data breach – has carved a wide trail of substantial consumer harm and injuries to consumers across the United States. Illustrative examples include:

a. Plaintiff Brystal Keller is a mother of five children who resides in Springfield, Missouri. Ms. Keller's prepaid Walmart GE Capital Visa debit card was compromised as a result of the Target data breach after Ms. Keller shopped at a Target store in Missouri during the data breach period. Ms. Keller learned that her card was compromised when

she attempted a withdrawal from an ATM and her card was declined. Ms. Keller had a fraudulent charge of $434.15 on her account from an unauthorized purchase by an unknown person made at a Target store in New York on December 26, 2013. Another fraudulent charge in the amount of $276 appeared on Ms. Keller's card as a result of an unauthorized charge made in Lawson, South Carolina, also on December 26, 2013. Ms. Keller's bank did not reimburse either fraudulent charge until January 7, 2014, more than two weeks after the fraud occurred. Ms. Keller had direct deposit set up and she was locked out of her account from December 26, 2013 until January 21, 2014. As a result of her account being frozen, Ms. Keller was unable to pay three bills, resulting in Ms. Keller incurring multiple, unreimbursed late fees. Ms. Keller relied upon her prepaid card as her primary source of payment. As a result of the Target data breach and the resulting loss of access to her account funds, Ms. Keller missed a rent payment, a car loan payment, and a washer and dryer payment, resulting in unreimbursed fees of $150, $34 and $15, respectively. As a result of the Target data breach, Ms. Keller had difficulty putting food on the table for her family during the holidays.

b. Plaintiff Aimee King is a resident of Sacramento, California, who, after using her Meta Bank Visa debit card to shop at Target in California during the period of the breach, had seven unauthorized charges on her bank account totaling approximately $940. During this time, Ms. King's husband was unemployed and she was the sole income earner for her family. The family greatly relied upon her bank account. Due to the Target data breach and the resulting unauthorized charges on her account, Ms. King was unable to pay her bills, including her car insurance, rent, loan, and cell phone bills. As a result, she incurred about $275 in late fees that were not reimbursed. Ms. King had to borrow money from her mother to cover rent and the interest rate on her loan increased from 50% to 175%. Additionally, Ms. King's

credit score dropped by approximately 40 points, disrupting her plan to purchase a car because she could not obtain financing at an affordable interest rate. Ms. King also spent significant time completing dispute documents with the bank and resetting automatic payment instructions for accounts linked to her bank account.

c. Plaintiff Christie Oliver, a resident of Spring, Texas, used her Bank of America Visa debit card to purchase goods at a Target store in Texas during the Target data breach. Plaintiff Oliver's personal information associated with her debit card was compromised in and as a result of the Target data breach. When Ms. Oliver's card was declined on December 22, 2013, Ms. Oliver discovered unauthorized charges on her account totaling $1,506.98. Ms. Oliver's bank account was partially frozen and she was able to access only about $700 of her account funds until December 31, 2013, when her bank released her account funds. Ms. Oliver had no money to complete her Christmas and grocery shopping, and she was unable to host Christmas dinner. During the time when families gather, Ms. Oliver was unable to visit or buy presents for her grandchildren, ages five and seven. She experienced her worst holiday ever. Moreover, Ms. Oliver was unable to make her mortgage payment on time and, as a result, incurred a late fee, which has not been reimbursed. Ms. Oliver also spent time resetting automatic payment instructions for her accounts and was assessed new (replacement) check fees, which were not reimbursed.

d. Plaintiff Deborah Rhodes, who resides in Streetsboro, Ohio, used her GE Capital Visa debit card to make purchases at Target in Ohio during the data breach period. Ms. Rhodes' personal information associated with her credit card was compromised in and as a result of the Target breach. Ms. Rhodes incurred an unauthorized charge on her account of $3,900 from a purchase by an unknown person at a Target store located in New York. Because of the

unauthorized charges, Ms. Rhodes account, which she shares with her husband, had a negative balance of $3,600. Ms. Rhodes receives disability payments and Mr. Rhodes is paid via direct deposit. Ms. Rhodes and her husband were not able to access their needed funds because their account was frozen by their bank which resulted in missed bill payments and subsequent late fees. As a result of the Target breach, Ms. Rhodes and her husband were compelled to file a police report and forced to borrow money for two weeks in order to meet daily living needs. Ms. Rhodes purchased credit monitoring services from AAA, for which she pays $70 per month in fees. Ms. Rhodes has not been reimbursed for card replacement fees or for late fees imposed as a result of their inability to make bill payments.

e. Plaintiff Michelle Mannion is a single mother of three children who lives and works as a psychiatric nurse in Amherst, Ohio. Ms. Mannion discovered that her Lorain National Bank MasterCard debit card, which she had used to make purchases at a Target store in Ohio during the Target data breach period, was compromised when she attempted to make a purchase for which the card covered only a certain amount and she had to pay the balance in cash. Upon contacting her bank, Ms. Mannion discovered four unauthorized charges totaling approximately $222 had been made to her account. Ms. Mannion's account was frozen by her bank. As a result, Ms. Mannion's plans to celebrate her daughter's 21st birthday on December 22, 2013 were spoiled. Ms. Mannion's holiday was ruined as she lacked access to her account and worried about how to feed her children until her next paycheck. Ms. Mannion recalls breaking out in tears after learning that her account was drained.

f. Plaintiff Frederick Smart is a resident of Little Elm, Texas and father of five who used his Chase Bank Visa debit card and Target REDcard debit card to purchase goods at a Target in Texas during the data breach period. Plaintiff Smart's personal information

associated with his debit card and Target REDcard debit card was compromised in and as a result of the Target data breach. Soon after making purchases at Target, Mr. Smart incurred fraudulent charges on his debit card totaling approximately $277 in December 2013. Plaintiff Smart also incurred unauthorized charges on his Target REDcard debit card totaling approximately $101 in November 2013. Following the Target data breach, scammers opened multiple phony accounts in Mr. Smart's name and attempted to open many other accounts. Plaintiff Smart experienced a loss of access to his funds and had restrictions placed on his account as a result of the Target data breach. After approximately 35 fraudulent inquiries on his credit bureau records, Mr. Smart's credit score dropped approximately 25 to 50 points. Because of this diminished credit score, Mr. Smart had to delay purchase of a new car. As a result of the Target data breach, Mr. Smart has received numerous scam telephone calls and mail and has purchased extensive credit monitoring services. Mr. Smart also spent time resetting automatic payment instructions for his accounts, incurred late payment fees due to failed automatic payments, and paid a replacement card fee as a result of the Target data breach.

g. Plaintiff Martha Reynoso is a resident of Chicago, Illinois, who, after using her EPPICard debit card at a Target store in Illinois during the Target data breach, had her EPPICard account almost entirely depleted in a series of international ATM transactions. Within a few minutes on December 28, 2013, the balance in Ms. Reynoso's account was depleted from $3,643.53 to $5.86, as a result of five international ATM transactions by an unauthorized person. The unauthorized charges included an international transaction fee of $24.92 and an international withdrawal fee of $1.25 for each of the five withdrawals. The EPPICard is used by the state of Illinois to facilitate the payment of child support, which Ms. Reynoso was receiving from her ex-husband for the care of her son. The large unauthorized withdrawals (in the amount of $830.51

for the first four withdrawals and $199.32 for the fifth one), all made outside of the United States, were grossly at odds with Ms. Reynoso's spending using her EPPICard, which were for purchases in Illinois, and for much smaller amounts. The unauthorized charges were also extremely unusual given the nature of Ms. Reynoso's EPPICard plan for child support. Ms. Reynoso first heard about the Target Breach on the news. On December 28, 2013 she learned she had been affected when her EPPICard was declined for insufficient funds. Ms. Reynoso used the EPPICard to assist with expenses for her son, including groceries, school tuition, and other related expenses. As a result of the Target data breach, Ms. Reynoso's EPPICard account was frozen from December 28, 2013 until January 14, 2014, leaving her no source of funds to care for her son. Without other options, Ms. Reynoso was forced to borrow money from her brother and ex-husband, and depleted some of her savings in order to feed her son and cover his tuition payments. Ms. Reynoso was also forced to cut back on spending in order to make ends meet. In addition, Ms. Reynoso was forced to obtain a replacement EPPICard at a cost of $5 for which she was not reimbursed. The unauthorized withdrawals and associated international transaction and withdrawal fees were eventually reimbursed by Ms. Reynoso's bank.

Plaintiffs Brystal Keller, Aimee King, Christie Oliver, Deborah Rhodes, Michelle Mannion, Frederick Smart and Martha Reynoso would not have shopped at Target using their credit or debit cards—indeed, they would not have made purchases at all at Target during the Target security breach—had Target disclosed that it did not have adequate security to safeguard customers' financial and personal data, or had Target timely and accurately notified them of the Target data breach.

2. As a result of the Target data breach, the credit and debit card account information of 40 million Target customers, as well as the personal information of 70 million

Target customers, has been exposed to fraud and these 110 million customers have been harmed. The injuries suffered by Consumer Plaintiffs and the proposed Classes as a direct result of the Target data breach include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Target data breach in the weeks leading up to and beyond the end-of-year holiday season;

f. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Consumer Plaintiffs' and Class members' information on the Internet card black market;

g. damages to and diminution in value of their personal and financial information entrusted to Target for the sole purpose of purchasing products from Target and with the mutual understanding that Target would safeguard Consumer Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. money paid for products purchased at Target stores during the period of the Target data breach in that Consumer Plaintiffs and Class members would not have shopped at Target had Target disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Target provided timely and accurate notice of the Target data breach;

i. overpayments paid to Target for products purchased during the Target data breach in that a portion of the price for such products paid by Consumer Plaintiffs and the Class to Target was for the costs of Target providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Target did not do, and as a result, Consumer Plaintiffs and members of the Class did not receive what they paid for and were overcharged by Target; and

j. continued risk to their financial and personal information, which remains in the possession of Target and which is subject to further breaches so long as Target fails to undertake appropriate and adequate measures to protect Consumer Plaintiffs' and Class members' data in its possession.

3. Consumer Plaintiffs seek to remedy these harms, and prevent their future occurrence, on behalf of themselves and all similarly situated consumers whose account and/or personally identifying information was stolen as a result of the Target data breach. Consumer Plaintiffs assert claims against Target for violations of state consumer laws, state data breach statutes, negligence, breach of implied contract, breach of the Target REDcard debit card contract, bailment and unjust enrichment. On behalf of themselves and all similarly situated consumers, Consumer Plaintiffs seek to recover damages, including actual and statutory damages, and equitable relief, including injunctive relief to prevent a reoccurrence of the data breach, restitution, disgorgement and costs and reasonable attorney fees.

II. JURISDICTION AND VENUE

4. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

5. This Court has jurisdiction over Target because the company maintains its principal place of business in Minnesota, regularly conducts business in Minnesota and has sufficient minimum contacts in Minnesota. Target intentionally avails itself of this jurisdiction by marketing and selling products from Minnesota to millions of consumers nationwide, including in Minnesota.

6. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Consumer Plaintiffs' claims occurred in this District.

III. PARTIES

7. Consumer Plaintiffs, including the Consumer Plaintiffs identified in paragraphs 1 and 8-112, and the proposed Classes include all persons in the United States whose credit or debit card information and/or whose personal information was compromised as a result of the Target data breach first disclosed by Target on December 19, 2013.

8. Plaintiff Kethra Ramert ("Plaintiff Ramert"), a resident of Anchorage, Alaska, used her Target REDcard debit card and Bank of America Visa credit card to purchase goods at a Target store in Alaska during the period of the Target data breach. Plaintiff Ramert's financial and personal information associated with her Target REDcard was compromised in and as a result of the Target data breach. Plaintiff Ramert was harmed by having her financial and personal information compromised. She incurred three unauthorized charges of approximately $100, $13, and $14 in January 2014. Plaintiff Ramert's personal information associated with her Visa credit card was also compromised in and as a result of the Target data breach. She also experienced a loss of access to her funds as a result of the Target data breach.

9. Plaintiff Susan Ryals ("Plaintiff Ryals"), a resident of Montgomery, Alabama, used her Max Credit Union Visa to purchase goods at a Target store in Alabama during the period of the Target data breach. Plaintiff Ryals' personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Ryals was harmed by having her financial and personal information compromised. She incurred two unauthorized

charges of approximately $108 and $20 on July 18, 2014. Plaintiff Ryals also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

10. Plaintiff Heather Herring ("Plaintiff Herring"), a resident of Pike Road, Alabama, used her Regent Bank Visa debit card and her Toys 'R Us MasterCard credit card to purchase goods at a Target store in Alabama during the period of the Target data breach. Plaintiff Herring's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Herring was harmed by having her financial and personal information compromised. She incurred two unauthorized charges on her MasterCard credit card of approximately $3 and $800 on December 24, 2013. Plaintiff Herring also experienced a loss of access to her funds associated with her MasterCard credit card. Plaintiff Herring's personal information associated with her Visa debit card was also compromised and she spent time resetting automatic payment instructions for her accounts. She also paid for credit monitoring services as a result of the Target data breach.

11. Plaintiff Joseph Madison ("Plaintiff Madison"), a resident of Deatsville, Alabama, used his PNC Visa debit card to purchase goods at a Target store in Alabama during the period of the Target data breach. Plaintiff Madison's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Madison was harmed by having his financial and personal information compromised. He incurred two unauthorized charges of approximately $822 and $444 on December 18, 2014. He also experienced three attempted unauthorized charges of $150 to his bank account. Plaintiff Madison also spent time completing a police report and resetting automatic payment instructions for his accounts as a result of the Target data breach.

12. Plaintiff Marilyna Kelly ("Plaintiff Kelly"), a resident of Midland City, Alabama, used her Army Aviation Federal Credit Union MasterCard debit card to purchase goods at a Target store in Alabama during the period of the Target data breach. Plaintiff Kelly's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Kelly was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Kelly also experienced a loss of access to her funds and was compelled to borrow money to cover her expenses. She also spent time resetting automatic payment instructions for her accounts and incurred late payment fees due to missed payments as a result of the Target data breach.

13. Plaintiff Cynthia Polk ("Plaintiff Polk"), a resident of Little Rock, Arkansas, used her Bank of America Visa debit card to purchase goods at a Target store in Arkansas during the period of the Target data breach. Plaintiff Polk's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Polk was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Polk also experienced a loss of access to her funds and spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

14. Plaintiff Cheryl Rogers ("Plaintiff Rogers"), a resident of Mesa, Arizona, used her Altura Credit Union Visa debit card to purchase goods at a Target store in Arizona during the

period of the Target data breach. Plaintiff Rogers' personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Rogers was harmed by having her financial and personal information compromised. She incurred an unauthorized charge of approximately $33 on February 20, 2014. Plaintiff Rogers also experienced a loss of access to her funds and spent time resetting automatic payment instructions for her accounts. She also spent time completing a police report and affidavit for the bank as a result of the Target data breach.

15. Plaintiff Dennis Gleine ("Plaintiff Gleine"), a resident of Phoenix, Arizona, used his Chase Bank MasterCard credit card to purchase goods at a Target store in Arizona during the period of the Target data breach. Plaintiff Gleine's personal information associated with his credit card was compromised in and as a result of the Target data breach. Plaintiff Gliene was harmed by having his financial and personal information compromised. He incurred an unauthorized charge of approximately $396 on January 9, 2014. Plaintiff Gliene also experienced a loss of access to his funds and spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

16. Plaintiff Terry Dorsch ("Plaintiff Dorsch"), a resident of Peoria, Arizona, used his Chase Bank Visa debit card to purchase goods at a Target store in Illinois during the period of the Target data breach. Plaintiff Dorsch's debit card was compromised in and as a result of the Target data breach. Plaintiff Dorsch was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Dorsch also experienced identity theft when his social security number was stolen and

used to open a new bank account and file a fraudulent tax return. As a result, Plaintiff Dorsch was compelled to file a police report and paperwork with the Arizona Attorney General. Plaintiff Dorsch was also compelled to contact multiple credit bureaus, the United States Secret Service, and all banks and credit card companies involved in the theft as a result of the Target data breach.

17. Plaintiff Gregory Ford ("Plaintiff Ford"), a resident of Mesa, Arizona, used his First Bank of Arizona Visa debit card and Capitol One MasterCard credit card to purchase goods at a Target store in Arizona during the period of the Target data breach. Plaintiff Ford's debit and credit cards were compromised in and as a result of the Target data breach. Plaintiff Ford was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Ford also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

18. Plaintiff Thomas Dorobiala ("Plaintiff Dorobiala"), a resident of Temecula, California, used his Navy Federal Credit Union Visa debit card, Navy Federal Credit Union Visa credit card, and Target REDcard debit card to purchase goods at a Target store in California during the Target data breach. Plaintiff Dorobiala's personal information associated with his Visa credit card was compromised in and as a result of the Target data breach. Plaintiff Dorobiala was harmed by having his financial and personal information compromised. He experienced three instances of attempted unauthorized charges to his account totaling approximately $630 in December 2013. He also experienced a loss of access to his funds on his Visa credit card. Plaintiff Dorobiala's personal information associated with his debit cards was

also compromised in and as a result of the Target data breach. He paid for credit monitoring services as a result of the Target data breach.

19. Plaintiff Christopher Boasso ("Plaintiff Boasso"), a resident of Petaluma, California, used his Bank of America Visa debit card, Chase Bank Visa debit card, and Chase Capital One Visa credit card to purchase goods at a Target store in California during the period of the Target data breach. Plaintiff Boasso's personal information associated with his Bank of America debit card was compromised in and as a result of the Target data breach. Plaintiff Boasso was harmed by having his financial and personal information compromised. He incurred four unauthorized charges of approximately $1003, $200, $800, and $1003 in December 2013. He also experienced a loss of access to his funds and spent time resetting automatic payment instructions for his accounts. Plaintiff Dorobiala's personal information associated with his Chase Bank debit card and credit card was also compromised in and as a result of the Target data breach. He also paid for credit monitoring services as a result of the Target data breach.

20. Plaintiff Julie Melnichuk ("Plaintiff Melnichuk"), a resident of Oakland, California, used her Nordstrom Visa credit card and Citibank debit card to purchase goods at a Target store in California during the period of the Target data breach. Plaintiff Melnichuk's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Melnichuk was harmed by having her financial and personal information compromised. She incurred approximately ten unauthorized charges after her credit card information was compromised, experienced a loss of access to her account and incurred unreimbursed interest on the unauthorized charges as a result of the Target data breach. Plaintiff Melnichuk's personal information associated with her Citibank debit card was also compromised in and as a result of the Target data breach. She experienced a loss of access to her account,

incurred unreimbursed late payment fees due to failed automatic payments, and ended up closing her account as a result of the Target data breach.

21. Plaintiff Sami Eshtiyag ("Plaintiff Eshtiyag"), a resident of San Diego, California, used his Chase Bank Visa debit card to purchase goods at a Target store in California during the period of the Target data breach. Plaintiff Eshtiyag's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Eshtiyag was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Eshtiyag also experienced a loss of access to his funds, spent time resetting automatic payment instructions for his accounts, and paid for credit monitoring services as a result of the Target data breach.

22. Plaintiff Brian Parit Smith ("Plaintiff Smith"), a resident of Novato, California, used his USAA Federal Savings Visa debit card to purchase goods at a Target store in California during the period of the Target data breach. Plaintiff Smith's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Smith was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Smith also experienced a loss of access to his funds and spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

23. Plaintiff Rosemary Cueva ("Plaintiff Cueva"), a resident of Vacaville, California, used her Wells Fargo Visa debit card to purchase goods at a Target store in California during the period of the Target data breach. Plaintiff Cueva's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Cueva was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Cueva also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

24. Plaintiff Corey Abels ("Plaintiff Abels"), a resident of Aurora, Colorado, used his Compass Bank Visa debit card to purchase goods at a Target store in Colorado during the period of the Target data breach. Plaintiff Abels' personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Abels was harmed by having his financial and personal information compromised. He experienced an attempted unauthorized charge to his bank account in December 2013. Plaintiff Abels also experienced a loss of access to his funds as a result of the Target data breach.

25. Plaintiff Bryan Council ("Plaintiff Council"), a resident of Highlands Ranch, Colorado, used his Wells Fargo Visa debit card and Chase Bank Visa credit card to purchase goods at a Target store in Colorado during the period of the Target data breach. Plaintiff Council's personal information associated with his debit and credit card was compromised in and as a result of the Target data breach. Plaintiff Council was harmed by having his financial and personal information compromised. He experienced an attempted unauthorized charge to his bank account on December 31, 2013. Plaintiff Council also experienced attempted identity theft

and as he received numerous phone calls from automobile and health insurance companies about fraudulent accounts set up with his personal information. Additionally, Plaintiff Council spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

26. Plaintiff Cathy Bok ("Plaintiff Bok"), a resident of Aurora, Colorado, used her Target REDcard debit card to purchase goods at a Target store in Colorado during the period of the Target data breach. Plaintiff Bok's personal information associated with her Wells Fargo bank account linked to her Target REDcard debit card was compromised in and as a result of the Target data breach. Plaintiff Bok was harmed by having her financial and personal information compromised. She experienced multiple instances of attempted unauthorized charges to her Wells Fargo credit card in January 2014. Plaintiff Bok lost access to her funds, spent time resetting automatic payment instructions for her accounts, and paid for credit monitoring services as a result of the Target data breach.

27. Plaintiff William Kurtz ("Plaintiff Kurtz"), a resident of Highlands Ranch, Colorado, used his Target REDcard debit card to purchase goods at a Target store in Colorado during the period of the Target data breach. Plaintiff Kurtz's personal information associated with his bank account linked to his Target REDcard debit card was compromised in and as a result of the Target data breach. Plaintiff Kurtz was harmed by having his financial and personal information compromised. He incurred unauthorized charges totaling approximately $545. Plaintiff Kurtz also lost access to his funds and spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

28. Plaintiff Linda Luby ("Plaintiff Luby"), a resident of Somers, Connecticut, used her American Eagle Federal Credit Union Visa debit card to purchase goods at a Target store in

Connecticut during the period of the Target data breach. Plaintiff Luby's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Luby was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Luby also lost access to her funds and spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

29. Plaintiff Vartouhi Kempe ("Plaintiff Kempe"), a resident of Brookfield, Connecticut, used her Citibank MasterCard credit card to purchase goods at a Target store in Connecticut during the period of the Target data breach. Plaintiff Kempe's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Kempe was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Kempe also lost access to her funds and spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

30. Plaintiff Scott Savedow ("Plaintiff Savedow"), a resident of Sunrise, Florida, used his Bright Star Credit Union Visa debit card to purchase goods at a Target store in Florida during the period of the Target data breach. Plaintiff Savedow's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Savedow was harmed by having his financial and personal information compromised. He incurred five

unauthorized charges totaling approximately $752 in December 2013. Plaintiff Savedow also experienced a loss of access to his funds as a result of the Target data breach.

31. Plaintiff Stephen Lagano ("Plaintiff Lagano"), a resident of Lighthouse Point, Florida, used his Bank of America Visa debit card to purchase goods at a Target store in Florida during the period of the Target data breach. Plaintiff Lagano's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Lagano was harmed by having his financial and personal information compromised. He incurred unauthorized charges totaling approximately $402 in December 2013. Plaintiff Lagano also experienced a loss of access to his funds as a result of the Target data breach.

32. Plaintiff Genevieve Edwards ("Plaintiff Edwards"), a resident of Guyton, Georgia, used her Savannah State Bank Visa debit card to purchase goods at a Target store in Georgia during the period of the Target data breach. Plaintiff Edwards's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Edwards was harmed by having her financial and personal information compromised. She incurred multiple unauthorized charges totaling approximately $1900 in December 2013. Plaintiff Edwards also experienced a loss of access to her funds, paid a replacement card fee for which she remains unreimbursed, and incurred late payment fees due to failed automatic payments. She also paid for credit monitoring services as a result of the Target data breach.

33. Plaintiff Abda Quillian ("Plaintiff Quillian"), a resident of Savannah, Georgia, used her Savannah State Bank Visa debit card to purchase goods at a Target store in Georgia during the period of the Target data breach. Plaintiff Quillian's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff

Quillian was harmed by having her financial and personal information compromised. She incurred multiple unauthorized charges totaling approximately $5,600 in January 2014, for which she was not fully-reimbursed. Plaintiff Quillian also experienced a loss of access to her funds, spent time completing multiple affidavits for the bank, resetting automatic payment instructions for her accounts, and incurred late payment fees due to failed automatic payments as a result of the Target data breach.

34. Plaintiff Misty Ellington ("Plaintiff Ellington"), a resident of Kennesaw, Georgia, used her Target REDcard debit card to purchase goods at a Target store in Georgia during the period of the Target data breach. Plaintiff Ellington's personal information associated with her Bank of America account linked to her Target REDcard debit card was compromised in and as a result of the Target data breach. Plaintiff Ellington was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Ellington also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

35. Plaintiff Heidi Bertucci ("Plaintiff Bertucci"), a resident of Honolulu, Hawaii, used her Target REDcard credit card to purchase goods at a Target store in Hawaii during the period of the Target data breach. Plaintiff Bertucci's personal information associated with her card was compromised in and as a result of the Target data breach. Plaintiff Bertucci was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity

theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

36. Plaintiff Bruce Fowler ("Plaintiff Fowler"), a resident of Sioux City, Iowa, used his Target Visa REDcard credit card and Wells Fargo Visa debit card to purchase goods at a Target store in Iowa during the period of the Target data breach. Plaintiff Fowler's personal information associated with his Target Visa REDcard (credit) and debit card was compromised in and as a result of the Target data breach. Plaintiff Fowler was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals.

37. Plaintiff Jason Liston ("Plaintiff Liston"), a resident of West Des Moines, Iowa, used his USAA Federal Savings Bank MasterCard debit card to purchase goods at a Target store in Iowa during the period of the Target data breach. Plaintiff Liston's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Liston was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Liston also experienced a loss of access to his funds and paid a replacement card fee for which he remains unreimbursed. He also spent time resetting automatic payment instructions for his accounts and incurred late payment fees due to failed automatic payments as a result of the Target data breach.

38. Plaintiff Patrick Mackey ("Plaintiff Mackey"), a resident of Mountain Home, Idaho, used his USAA Federal Savings Bank MasterCard debit card to purchase goods at a

Target store in Idaho during the period of the Target data breach. Plaintiff Mackey's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Mackey was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Mackey also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

39. Plaintiff Herminia Dolemba ("Plaintiff Dolemba"), a resident of Blue Island, Illinois, used her Fifth Third Bank MasterCard debit card to purchase goods at a Target store in Illinois during the period of the Target data breach. Plaintiff Dolemba's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Dolemba was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Dolemba also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

40. Plaintiff Stephen Papka ("Plaintiff Papka"), a resident of Champaign, Illinois, used his University of Illinois Employees Credit Union Visa debit card to purchase goods at a Target store in Illinois during the during the period of the Target data breach. Plaintiff Papka's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Papka was harmed by having his financial and personal information

compromised. He incurred ten unauthorized charges totaling approximately $315 in December 2013. Plaintiff Papka also experienced a loss of access to his funds, spent time completing dispute forms for his bank and resetting automatic payment instructions for his accounts as a result of the Target data breach.

41. Plaintiff Stan Sountharavong ("Plaintiff Sountharavong"), a resident of Belvidere, Illinois, used his BMO Harris Bank MasterCard debit card to purchase goods at a Target store in Illinois during the period of the Target data breach. Plaintiff Sountharavong's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Sountharavong was harmed by having his financial and personal information compromised. He incurred nine unauthorized charges totaling approximately $315 in February 2014. Plaintiff Sountharavong also experienced a loss of access to his funds and spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

42. Plaintiff Darcy Norder ("Plaintiff Norder"), a resident of Indianapolis, Indiana, used her Forum Credit Union MasterCard debit card to purchase goods at a Target store in Indiana during the period of the Target data breach. Plaintiff Norder's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Norder was harmed by having her financial and personal information compromised. She incurred fifteen unauthorized charges of approximately $1000 in January 2014. Plaintiff Norder also experienced a loss of access to her funds and spent time completing affidavits for her bank as a result of the Target data breach.

43. Plaintiff Lisa DeVito ("Plaintiff DeVito"), a resident of Bloomington, Indiana, used her Visa EPPICard debit card to purchase goods at a Target store in Indiana during the period of the Target data breach. Plaintiff DeVito's personal information associated with her

debit card was compromised in and as a result of the Target data breach. Plaintiff DeVito was harmed by having her financial and personal information compromised. She incurred unauthorized charges of approximately $240 in December 2013. Plaintiff DeVito also experienced a loss of access to her funds as a result of the Target data breach.

44. Plaintiff Pamela Eichorst ("Plaintiff Eichorst"), a resident of South Bend, Indiana, used her Wells Fargo Visa credit and debit cards to purchase goods at a Target store in Indiana during the period of the Target data breach. Plaintiff Eichorst's personal information associated with her credit and debit cards was compromised in and as a result of the Target data breach. Plaintiff Eichorst was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Eichorst also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

45. Plaintiff Valentina Ignatova ("Plaintiff Ignatova"), a resident of Kansas City, Kansas, used her Bank Midwest Visa debit card to purchase goods at a Target store in Kansas during the period of the Target data breach. Plaintiff Ignatova's card was compromised in and as a result of the Target data breach. Plaintiff Ignatova was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

46. Plaintiffs Jodi and David Schmidt ("Plaintiffs Schmidt"), residents of Olathe, Kansas, used their Commercial Bank debit card to purchase goods at a Target store in Kansas

during the period of the Target data breach. Plaintiffs' personal information associated with their debit card was compromised in and as a result of the Target data breach. Plaintiffs Schmidt were harmed by having their financial and personal information compromised. Plaintiffs Schmidt incurred two unauthorized charges of approximately $379 and $300 in December 2013. Plaintiffs' personal information associated with their card was also compromised in and as a result of the Target data breach. Plaintiffs Schmidt also experienced a loss of access to their account funds, spent time resetting automatic payment instructions for their accounts, and incurred declined payment fees as a result of the Target data breach.

47. Plaintiff Patricia Miller ("Plaintiff Patricia Miller"), a resident of Cold Spring, Kentucky, used her Fifth Third Bank MasterCard credit card to purchase goods at a Target store in Kentucky during the period of the Target data breach. Plaintiff Patricia Miller's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Patricia Miller was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Patricia Miller also experienced a loss of access to her funds and spent time resetting automatic payment instruction for her accounts as a result of the Target data breach.

48. Plaintiff Michelle Morales, ("Plaintiff Morales"), a resident of St. Joseph, Louisiana, used her Target Visa REDcard credit card to purchase goods at a Target store in Louisiana during the period of the Target data breach. Plaintiff Morales' personal information associated with her Target Visa REDcard credit card was compromised in and as a result of the Target data breach. Plaintiff Morales was harmed by having her financial and personal

information compromised. She incurred an unauthorized charge as a result of the Target data breach.

49. Plaintiff Eliza Huerta ("Plaintiff Huerta"), a resident of Mandeville, Louisiana, used her Navy Federal Credit Union Visa debit card to purchase goods at a Target store in Louisiana during the period of the Target data breach. Plaintiff Huerta's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Huerta was harmed by having her financial and personal information compromised. She incurred multiple unauthorized charges totaling approximately $1,000 in or around March 2013. Plaintiff Huerta also experienced a loss of access to her funds, spent time resetting automatic payment instructions for her accounts, and incurred late payment fees due to failed automatic payments as a result of the Target data breach.

50. Plaintiff Winston Casey ("Plaintiff Casey"), a resident of Dorchester, Massachusetts, used his Citibank MasterCard debit card to purchase goods at a Target store in Massachusetts during the period of the Target data breach. Plaintiff Casey's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Casey was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Casey also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

51. Plaintiff Mark Linscott, II ("Plaintiff Linscott"), a resident of Lowell, Massachusetts, used his Capital One MasterCard credit card to purchase goods at a Target store

in Massachusetts during the period of the Target data breach. Plaintiff Linscott's personal information associated with his credit card was compromised in and as a result of the Target data breach. Plaintiff Linscott was harmed by having his financial and personal information compromised. He incurred unauthorized charges of approximately $269, $249, and $3,697 in December 2013. Plaintiff Linscott experienced a loss of access to his funds, spent time resetting automatic payments for his accounts, and incurred unreimbursed late payment fees due to failed automatic payments as a result of the Target data breach. Plaintiff Linscott also experienced damage to his credit scores as a result of the Target data breach.

52. Plaintiff Nicole Alston ("Plaintiff Alston"), a resident of Glen Burnie, Maryland used her SunTrust Bank MasterCard debit card to purchase goods at a Target store in Maryland during the period of the Target data breach. Plaintiff Alston's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Alston also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

53. Plaintiff Lorne Murphy ("Plaintiff Murphy"), a resident of Lexington Park, Maryland, used his USAA MasterCard debit card to purchase goods at a Target store in Maryland during the period of the Target data breach. Plaintiff Murphy's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased

threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Murphy also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

54. Plaintiff Alexis Kowalcyk ("Plaintiff Kowalcyk"), a resident of Fenton, Michigan, used her Target REDcard to purchase goods at a Target store in Michigan during the period of the Target data breach. Plaintiff Kowalcyk's personal information associated with her Target REDcard was compromised in and as a result of the Target data breach. Plaintiff Kowalcyk was harmed by having her financial and personal information compromised. She incurred an unauthorized charge of approximately $455 on December 23, 2013. Plaintiff Kowalcyk experienced a loss of access to her funds and spent time resetting automatic payment instructions for her accounts. She was also compelled to borrow money to cover her expenses as a result of the Target data breach.

55. Plaintiff Michael Craig ("Plaintiff Craig"), a resident of Gross Pointe, Michigan, used his Chase Bank Visa debit card to purchase goods at a Target store in Michigan during the period of the Target data breach. Plaintiff Craig's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Craig was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Craig also experienced a loss of access to his funds, spent time resetting automatic payment instructions for his accounts and was compelled to borrow money to cover his expenses as a result of the Target data breach.

56. Plaintiff Steven Bensinger ("Plaintiff Bensinger"), a resident of Saugatuck, Michigan, used his Chase Bank Visa debit card and Chase Bank Visa credit card to purchase goods at a Target store in Michigan during the period of the Target data breach. Plaintiff Bensinger's personal information associated with his debit and credit cards was compromised in and as a result of the Target data breach. Plaintiff Bensinger was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Bensinger also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

57. Plaintiff Raymond Davis ("Plaintiff Davis"), a resident of Southfield, Michigan, used his Chase Bank Visa credit card to purchase goods at a Target store in Michigan during the period of the Target data breach. Plaintiff Davis' personal information associated with his credit card was compromised in and as a result of the Target data breach. Plaintiff Davis was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Davis also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

58. Plaintiff Roni Goldstein ("Plaintiff Goldstein"), a resident of Minneapolis, Minnesota, used her Wells Fargo Visa debit card to purchase goods at a Target store in Minnesota during the period of the Target data breach. Plaintiff Goldstein's personal information associated with her debit card was compromised in and as a result of the Target data

breach. Plaintiff Goldstein was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Goldstein also experienced a loss of access to her funds and spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

59. Plaintiff Sondra Morgan ("Plaintiff Morgan"), a resident of Houston, Minnesota, used her Wells Fargo Visa debit card to purchase goods at a Target store in Minnesota during the period of the Target data breach. Plaintiff Morgan's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Morgan was harmed by having her financial and personal information compromised. She incurred three unauthorized charges of approximately $5, $657, and $279 on January 27, 2014. Plaintiff Morgan also experienced a loss of access to her funds, spent time resetting automatic payment instructions for her accounts, and incurred unreimbursed late payment fees due to failed automatic payments as a result of the Target data breach.

60. Plaintiff Gloria Ransom ("Plaintiff Ransom"), a resident of Ballwin, Missouri, used her Discover credit card and Target Visa REDcard to purchase goods at a Target store in Missouri during the period of the Target data breach. Plaintiff Ransom's personal information associated with her cards was compromised in and as a result of the Target data breach. Plaintiff Ransom was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the

Internet black market and/or misused by criminals. Plaintiff Ransom also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

61. Plaintiff Jeanne Kirby ("Plaintiff Kirby"), a resident of St. Louis, Missouri, used her First Community Credit Union Visa credit card to purchase goods at a Target store in Missouri during the period of the Target data breach. Plaintiff Kirby's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Kirby was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Kirby also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

62. Plaintiff Amanda Stewart ("Plaintiff Stewart"), a resident of Saint Peters, Missouri, used her Citibank MasterCard credit card to purchase goods at a Target store in Missouri during the period of the Target data breach. Plaintiff Stewart's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Stewart was harmed by having her financial and personal information compromised. She incurred four unauthorized charges in December 2013. She also experienced multiple instances of attempted unauthorized charges to her credit card account. Plaintiff Stewart also experienced a loss of access to her funds and spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

63. Plaintiff Barbara Donald ("Plaintiff Donald"), a resident of Jackson, Mississippi, used her H&R Block Emerald prepaid card to purchase goods at a Target store in Mississippi

during the period of the Target data breach. Plaintiff Donald's personal information associated with her prepaid card was compromised in and as a result of the Target data breach. Plaintiff Donald was harmed by having her financial and personal information compromised and incurred multiple unauthorized charges to her account in December 2013. Plaintiff Donald experienced a loss of access to her funds, incurred unreimbursed late fees for missed payments, and had household utilities shut off because she had no access to her money as a result of the Target data breach. She was unable to pay her mortgage and had to refinance her home loan. Plaintiff Donald was also compelled to borrow money to cover her living expenses as a result of the Target data breach.

64. Plaintiff Janice Kisner ("Plaintiff Kisner"), a resident of Oxford, Mississippi, used her First National Bank of Oxford MasterCard debit card to purchase goods at a Target store in Mississippi during the period of the Target data breach. Plaintiff Kisner's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Kisner was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

65. Plaintiff Cheryl Miller ("Plaintiff Cheryl Miller"), a resident of Billings, Montana, used her Rocky Mountain Bank Visa debit card to purchase goods at a Target store in Montana during the period of the Target data breach. Plaintiff Cheryl Miller's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Cheryl Miller was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm

from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

66. Plaintiff Anita Simonsen ("Plaintiff Simonsen"), a resident of Billings, Montana, used her Rocky Mountain Visa debit card to purchase goods at a Target store in Montana during the period of the Target data breach. Plaintiff Simonsen's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Simonsen was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

67. Plaintiff Jean Wilson ("Plaintiff Wilson"), a resident of Charlotte, North Carolina, used her US Airways Barclays Bank MasterCard credit card to purchase goods at a Target store in North Carolina during the period of the Target data breach. Plaintiff Wilson's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Wilson was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Wilson also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

68. Plaintiff Marion Lovelace ("Plaintiff Lovelace"), a resident of Kernersville, North Carolina, used her Target REDcard debit card to purchase goods at a Target store in North Carolina during the period of the Target data breach. Plaintiff Lovelace's personal information

associated with her Target REDcard was compromised in and as a result of the Target data breach. Plaintiff Lovelace was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Lovelace also paid for credit monitoring services as a result of the Target data breach.

69. Plaintiff Michelle Bryant ("Plaintiff Bryant"), a resident of Rockwell, North Carolina, used her Target REDcard debit card to purchase goods at a Target store in North Carolina and Virginia during the Target data breach. Plaintiff Bryant's personal information associated with her Target REDcard was compromised in and as a result of the Target data breach. Plaintiff Bryant was harmed by having her financial and personal information compromised. She experienced fraud and unauthorized activity totaling approximately $2,400 in her primary savings account and unauthorized activity totaling approximately $1,500 in a secondary savings account, which were linked to the Target REDcard. Plaintiff Bryant experienced a loss of access to her funds, spent time resetting automatic payment instructions for her accounts, and incurred late payment fees due to failed automatic payments as a result of the Target data breach. Plaintiff Bryant also paid for credit monitoring services as a result of the Target data breach.

70. Plaintiff Jerron Knox ("Plaintiff Knox"), a resident of Charlotte, North Carolina used his Bancorp Visa debit card to purchase goods at a Target store in North Carolina during the period of the Target data breach. Plaintiff Knox's personal information associated with his Bancorp Visa debit card was compromised in and as a result of the Target data breach. Plaintiff Knox was harmed by having his financial and personal information compromised. He incurred

two unauthorized charges totaling approximately $164 in January 2014. Plaintiff Knox experienced a loss of access to his funds which resulted in late fees and was compelled to borrow money to cover his living expenses as a result of the Target data breach.

71. Plaintiff Alissa Farol ("Plaintiff Farol"), a resident of Fargo, North Dakota, used her Postal Family Credit Union debit card to purchase goods at a Target store in North Dakota during the period of the Target data breach. Plaintiff Farol's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Farol was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Farol experienced a loss of access to her funds as a result of the Target data breach.

72. Plaintiff Matthew Marciniak ("Plaintiff Marciniak"), a resident of Bellevue, Nebraska, used his Wells Fargo Visa debit card to purchase goods at a Target store in Nebraska during the period of the Target data breach. Plaintiff Marciniak's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Marciniak was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Marciniak also paid for credit monitoring services as a result of the Target data breach.

73. Plaintiff Kami Raleigh ("Plaintiff Raleigh"), a resident of Manchester, New Hampshire, used her Peoples United Bank MasterCard debit card to purchase goods at a Target

store in New Hampshire during the period of the Target data breach. Plaintiff Raleigh's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Raleigh was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Raleigh also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

74. Plaintiff Tasha Boykin ("Plaintiff Boykin"), a resident of Hackettstown, New Jersey, used her Amerifirst Bank MasterCard debit card to purchase goods at a Target store in New Jersey during the period of the Target data breach. Plaintiff Boykin's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Boykin was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Boykin also experienced a loss of access to her funds and paid for credit monitoring services as a result of the Target data breach.

75. Plaintiff Andrew Rosenberg ("Plaintiff Rosenberg"), a resident of Livingston, New Jersey, used his American Express credit card to purchase goods at a Target store in New Jersey during the period of the Target data breach. Plaintiff Rosenberg's personal information associated with his credit card was compromised in and as a result of the Target data breach. Plaintiff Rosenberg was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the

increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Rosenberg experienced multiple instances of attempted unauthorized charges to his credit card. He also experienced a loss of access to his funds and spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

76. Plaintiff Sharon Sanders ("Plaintiff Sanders"), a resident of Rockaway, New Jersey, used her Target REDcard (credit) to purchase goods at a Target store in New Jersey during the period of the Target data breach. Plaintiff Sanders' personal information associated with her card was compromised in and as a result of the Target data breach. Plaintiff Sanders was harmed by having her financial and personal information compromised. She incurred an unauthorized charge of approximately $1800 in December 2013. Plaintiff Sanders also experienced a loss of access to her credit as a result of the Target data breach.

77. Plaintiff Lynda Fazio ("Plaintiff Fazio"), a resident of Albuquerque, New Mexico, used her New Mexico Bank and Trust Visa debit card to purchase goods at a Target store in New Mexico during the period of the Target data breach. Plaintiff Fazio's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Fazio was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Fazio also paid a replacement card fee and an overdraft fee for which she remains unreimbursed as a result of the Target data breach.

78. Plaintiff Kenneth Coca ("Plaintiff Coca"), a resident of Las Vegas, Nevada, used his Capitol One MasterCard credit card and Wells Fargo Visa credit and debit card to purchase goods at a Target store in Nevada during the period of the Target data breach. Plaintiff Coca's personal information associated with his debit and credit cards was compromised in and as a result of the Target data breach. Plaintiff Coca was harmed by having his financial and personal information compromised. He experienced multiple instances of attempted unauthorized charges to his Wells Fargo credit card. He also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

79. Plaintiff Tracy Brigida ("Plaintiff Brigida"), a resident of Las Vegas, Nevada, used her Chase Bank Visa debit card and Target REDcard credit card to purchase goods at a Target store in Nevada during the period of the Target data breach. Plaintiff Brigida's personal information associated with her credit and debit cards was compromised in and as a result of the Target data breach. Plaintiff Brigida was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Brigida also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

80. Plaintiff Eric Keller ("Plaintiff Keller"), a resident of Carson City, Nevada, used his Greater Nevada Credit Union Visa debit card to purchase goods at a Target store in Nevada during the period of the Target data breach. Plaintiff Keller's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Keller was harmed by having his financial and personal information compromised. He incurred an

unauthorized charge in December 2013. Plaintiff Keller also experienced a loss of access to his funds and spent time resetting automatic payment instructions for his accounts. He also paid new check fees due to getting a new account number and paid to cancel three checks as a result of the Target data breach.

81. Plaintiff John Patrick Fahy ("Plaintiff Fahy"), a resident of Sanborn, New York, used his Navy Federal Credit Union MasterCard credit card to purchase goods at a Target store in New York during the period of the Target data breach. Plaintiff Fahy's personal information associated with his credit card was compromised in and as a result of the Target data breach. Plaintiff Fahy was harmed by having his financial and personal information compromised. He incurred unauthorized charges of approximately $509, $530, and $504 in January 2014. Plaintiff Fahy also experienced a loss of access his funds, damage to his credit score, and was required to file a police report as a result of the Target data breach.

82. Plaintiff Deborah Guercio ("Plaintiff Guercio"), a resident of Brooklyn, New York, used her Dime Savings Bank of Williamsburg Visa debit card to purchase goods at a Target store in New York during the period of the Target data breach. Plaintiff Guercio's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Guercio was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. After receiving a replacement debit card from her bank, Plaintiff Guercio had difficulty returning items to Target using her replacement card which resulted in her paying for unwanted merchandise.

Plaintiff Guercio also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

83. Plaintiff Martino Pietanza ("Plaintiff Pietanza"), a resident of Brooklyn, New York, used his Chase Bank Visa debit card to purchase goods at a Target store in New York during the period of the Target data breach. Plaintiff Pietanza's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Pietanza was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Pietanza also experienced a loss of access to his funds, had restrictions placed on his account, and spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

84. Plaintiff Leslie Wolff ("Plaintiff Wolff"), a resident of Brooklyn, New York, used her Chase Bank Visa debit card to purchase goods at a Target store in New York during the period of the Target data breach. Plaintiff Wolff's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Wolff was harmed by having her financial and personal information compromised. She experienced multiple instances of attempted unauthorized charges to her bank account. Plaintiff Wolff also experienced a loss of access to her funds and spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

85. Plaintiff Robert Jefferson ("Plaintiff Jefferson"), a resident of Cincinnati, Ohio, used his prepaid Visa Walmart MoneyCard debit card to purchase goods at a Target store in Ohio during the period of the Target data breach. Plaintiff Jefferson's personal information

associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Jefferson was harmed by having his financial and personal information compromised. He incurred unauthorized charges of approximately $541 and $172 in December 2013. Plaintiff Jefferson also paid a replacement card fee for which he remains unreimbursed and experienced a loss of access to his funds as a result of the Target data breach.

86. Plaintiff Terri Heilman-Keck ("Plaintiff Heilman-Keck"), a resident of Yukon, Oklahoma, used her IBC Bank Visa debit card to purchase goods at a Target store in Oklahoma during the period of the Target data breach. Plaintiff Heilman-Keck's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Heilman-Keck was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

87. Plaintiff Cynthia Noe ("Plaintiff Noe"), a resident of Glenpool, Oklahoma, attempted to use her City National Bank Visa debit card to purchase goods at a Target store in Oklahoma during the period of the Target data breach. After several unsuccessful attempted swipes of her debit card, Plaintiff Noe paid in cash for her items. Plaintiff Noe's personal and debit card information was nevertheless retained by Target and Plaintiff Noe's attempted purchases were reflected in her subsequent bank statements. As a result, Plaintiff Noe's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Noe was harmed by having her financial and personal information compromised. She incurred unauthorized charges of approximately $296 and $17 in December

2013. Plaintiff Noe also experienced a loss of access to her funds and paid for credit monitoring services as a result of the Target data breach.

88. Plaintiff John Meyers ("Plaintiff Meyers"), a resident of Tulsa, Oklahoma, used his Bank of America Visa debit card to purchase goods at a Target store in Oklahoma during the period of the Target data breach. Plaintiff Meyers' personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Meyers was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Meyers also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

89. Plaintiff Anay Hausner ("Plaintiff Hausner"), a resident of Sweet Home, Oregon, used her Chase Bank MasterCard debit card to purchase goods at a Target store in Oregon during the period of the Target data breach. Plaintiff Hausner's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Hausner was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Hausner also had her credit and ATM limits reduced and spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

90. Plaintiff Paul Jaroszewski ("Plaintiff Jaroszewski"), a resident of Portland, Oregon, used his Arizona Central Credit Union Visa debit card to purchase goods at a Target

store in Oregon during the period of the Target data breach. Plaintiff Jaroszewski's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Jaroszewski was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Jaroszewski also experienced a loss of access to his funds and spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

91. Plaintiff Misty Bearden ("Plaintiff Bearden"), a resident of Eugene, Oregon, used her Oregon Community Credit Union Visa debit card to purchase goods at a Target store in Oregon during the period of the Target data breach. Plaintiff Bearden's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Bearden was harmed by having her financial and personal information compromised. She incurred unauthorized charges of approximately $100 and $55 in December 2013. Plaintiff Bearden also experienced a loss of access to her funds, had to borrow money to cover her expenses, and incurred overdraft fees as a result of the Target data breach.

92. Plaintiff Julia Rossi ("Plaintiff Rossi"), a resident of Newville, Pennsylvania, used her Target REDcard debit card to purchase goods at a Target store in Pennsylvania during the period of the Target data breach. Plaintiff Rossi's personal information associated with her bank account linked to her Target REDcard debit card was compromised in and as a result of the Target data breach. Plaintiff Rossi was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information

being sold on the Internet black market and/or misused by criminals. Plaintiff Rossi also spent time resetting automatic payment instructions for her accounts and incurred late payment fees due to failed automatic payments as a result of the Target data breach.

93. Plaintiff Susan Levin ("Plaintiff Levin"), a resident of Newville, Pennsylvania, used her Target REDcard to purchase goods at a Target store in Pennsylvania during the period of the Target data breach. Plaintiff Levin's personal information associated with her bank account linked to her Target REDcard was compromised in and as a result of the Target data breach. Plaintiff Levin was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Levin also spent time resetting automatic payment instructions for her accounts and incurred late payment fees due to failed automatic payments as a result of the Target data breach.

94. Plaintiff Stephen Homa ("Plaintiff Homa"), a resident of Okatie, South Carolina, used his H&R Block MasterCard debit card to purchase goods at a Target store in South Carolina during the period of the Target data breach. Plaintiff Homa's personal information associated with his payment card was compromised in and as a result of the Target data breach. Plaintiff Homa was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Homa also experienced a loss of access to his funds and spent time resetting automatic payment instructions for his accounts as a result of the Target data breach. Plaintiff Homa has not been reimbursed for the lack of access to his own

account funds. Plaintiff Homa would not have used a payment card to make purchases at Target during the period of the Target data breach had Target disclosed that it lacked adequate computer systems and data security practices to safeguard customers' personal and financial information from theft, and had Target provided him with timely and accurate notice of the Target data breach.

95. Plaintiff David Dean ("Plaintiff Dean"), a resident of Highmore, South Dakota, used his Both First Interstate Bank MasterCard debit card to purchase goods at a Target store in South Dakota during the period of the Target data breach. Plaintiff Dean's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Dean was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Dean also spent time resetting automatic payment instructions for his accounts as a result of the Target data breach.

96. Plaintiff Amber Rippy ("Plaintiff Rippy"), a resident of Bethpage, Tennessee, used her Citizens Bank Visa debit card to purchase goods at a Target store in Tennessee during the period of the Target data breach. Plaintiff Rippy's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Rippy was harmed by having her financial and personal information compromised. She incurred extensive unauthorized charges following the Target data breach. Plaintiff Rippy also experienced a loss of access to her funds, had restrictions placed on her account, and spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

97. Plaintiff Jerry Crawford ("Plaintiff Crawford"), a resident of Arlington, Tennessee, used his SunTrust Bank MasterCard debit card to purchase goods at a Target store in Tennessee during the period of the Target data breach. Plaintiff Crawford's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Crawford was harmed by having his financial and personal information compromised. He incurred unauthorized charges totaling approximately $160 in December 2013. Plaintiff Crawford also experienced a loss of access to his funds as a result of the Target data breach.

98. Plaintiff Val Prickett ("Plaintiff Prickett"), a resident of Nolansville, Tennessee, used her Banana Republic GE Capital Visa credit card to purchase goods at a Target store in Tennessee during the period of the Target data breach. Plaintiff Prickett's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Prickett was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

99. Plaintiff Johnny Breaux ("Plaintiff Breaux"), a resident of Houston, Texas, used his PrimeWay Credit Union Visa debit card to purchase goods at a Target store in Texas during the period of the Target data breach. Plaintiff Breaux's personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Breaux was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black

market and/or misused by criminals. Plaintiff Breaux also experienced a loss of access to his funds as a result of the Target data breach.

100. Plaintiff Jason Knicely ("Plaintiff Knicely"), a resident of Tyler, Texas, used his Chase Bank Visa credit card to purchase goods at a Target store in Texas during the period of the Target data breach. Plaintiff Knicely's personal information associated with his credit card was compromised in and as a result of the Target data breach. Plaintiff Knicely was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Knicely also had restrictions placed on his account as a result of the Target data breach.

101. Plaintiff Timothy Burnett ("Plaintiff Burnett"), a resident of Layton, Utah, used his Target REDcard debit card to purchase goods at a Target store in Utah during the period of the Target data breach. Plaintiff Burnett's personal information associated with his bank account linked to his Target REDcard debit card was compromised in and as a result of the Target data breach. Plaintiff Burnett was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals.

102. Plaintiff Ted Groves ("Plaintiff Groves"), a resident of Clearfield, Utah, used his America First Credit Union Visa debit card to purchase goods at a Target store in Utah during the period of the Target data breach. Plaintiff Groves' personal information associated with his debit card was compromised in and as a result of the Target data breach. Plaintiff Groves was

harmed by having his financial and personal information compromised. He incurred unauthorized charges on his debit card of approximately $6, $17, and $24 in January 2014. Plaintiff Groves also experienced a loss of access to his funds as a result of the Target data breach.

103. Plaintiff Ronald Humphrey ("Plaintiff Humphrey"), a resident of Chesapeake, Virginia, used his Military Star Chase Bank MasterCard credit card to purchase goods at a Target store in Virginia during the period of the Target data breach. Plaintiff Humphrey's personal information associated with his credit card was compromised in and as a result of the Target data breach. Plaintiff Humphrey was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals.

104. Plaintiff Sylvia Lederman ("Plaintiff Lederman"), a resident of Casanova, Virginia, used her TD Bank Visa debit card to purchase goods at a Target store in Virginia during the period of the Target data breach. Plaintiff Lederman's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Lederman was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

105. Plaintiff Darine Barbour ("Plaintiff Barbour"), a resident of Culpeper, Virginia, used her BB&T Bank Visa debit card to purchase goods at a Target store in Virginia during the period of the Target data breach. Plaintiff Barbour's personal information associated with her

debit card was compromised in and as a result of the Target data breach. Plaintiff Barbour was harmed by having her financial and personal information compromised. She incurred unauthorized charges on her debit card of approximately $490 and $326 in December 2013. Plaintiff Barbour had restrictions placed on her account, spent time resetting automatic payment instructions for her accounts, and incurred late payment fees due to failed automatic payments as a result of the Target data breach.

106. Plaintiff Lois Williams ("Plaintiff Williams"), a resident of Virginia Beach, Virginia, used her Citibank MasterCard credit card to purchase goods at a Target store in Virginia during the period of the Target data breach. Plaintiff Williams' personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Williams was harmed by having her financial and personal information compromised. She incurred ten unauthorized charges totaling approximately $4,773 in December 2013. Plaintiff Williams experienced a loss of access to her funds and was compelled to borrow money to cover her expenses. She also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

107. Plaintiff Christie Del Nagro ("Plaintiff Del Nagro"), a resident of Seattle, Washington, used her Target REDcard debit card to purchase goods at a Target store in Washington during the period of the Target data breach. Plaintiff Del Nagro's personal information associated with her Target REDcard was compromised in and as a result of the Target data breach. Plaintiff Del Nagro was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and

personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Del Nagro paid for credit monitoring services as a result of the Target data breach.

108. Plaintiff Tony Rosellini ("Plaintiff Rosellini"), a resident of Fincrest, Washington, used his Chase Bank MasterCard debit card to purchase goods at a Target store in Washington during the period of the Target data breach. The personal information associated with the debit card, which was jointly held with his spouse Erika Fawn Cole-Rosellini, was compromised in and as a result of the Target data breach. Plaintiff Rosellini and his spouse were harmed by having their financial and personal information compromised and face the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to their financial and personal information being sold on the Internet black market and/or misused by criminals. They also experienced an attempted unauthorized charge to their debit card account and a loss of access to their account funds as a result of the Target data breach. Plaintiff Rosellini and his spouse also spent time resetting automatic payment instructions for their accounts and incurred late payment fees due to failed automatic payments as a result of the Target data breach.

109. Plaintiff Aimee Sutton ("Plaintiff Sutton"), a resident of Seattle, Washington, used her Boeing Employee Credit Union MasterCard debit card to purchase goods at a Target store in Washington during the period of the Target data breach. Plaintiff Sutton's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Sutton was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

110. Plaintiff Piper Moore ("Plaintiff Moore"), a resident of Huntington, West Virginia, used her Fifth Third Bank MasterCard debit card to purchase goods at a Target store in West Virginia during the period of the Target data breach. Plaintiff Moore's personal information associated with her card was compromised in and as a result of the Target data breach. Plaintiff Moore was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Moore also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

111. Plaintiff Mary Webb ("Plaintiff Webb"), a resident of Mt. Clare, West Virginia, used her H&R Block MasterCard debit card to purchase goods at a Target store in West Virginia during the period of the Target data breach. Plaintiff Webb's personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff was harmed by having her financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

112. Plaintiff Dovina Thomas ("Plaintiff Thomas"), was a resident of Milwaukee, Wisconsin during the period of the Target data breach and used her Chase Bank Visa debit card to purchase goods at a Target store in Wisconsin during that period. Plaintiff Thomas' personal information associated with her debit card was compromised in and as a result of the Target data breach. Plaintiff Thomas was harmed by having her financial and personal information

compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals. She experienced instances of attempted unauthorized charges to her bank account. Plaintiff Thomas also spent time resetting automatic payment instructions for her accounts as a result of the Target data breach.

113. Plaintiff Janice Meier ("Plaintiff Meier"), a resident of Chippewa Falls, Wisconsin, used her Capitol One Visa credit card to purchase goods at a Target store in Wisconsin during the period of the Target data breach. Plaintiff Meier's personal information associated with her credit card was compromised in and as a result of the Target data breach. Plaintiff Meier was harmed by having her financial and personal information compromised. She incurred unauthorized charges on her credit card of approximately $179 in February 2014. Plaintiff Meier experienced a loss of access to her funds and had restrictions placed on her account as a result of the Target data breach. Plaintiff Meier also spent time resetting automatic payment instructions for her accounts which resulted in late payments as a result of the Target data breach.

114. Consumer Plaintiffs would not have used their credit or debit cards to make purchases at Target—indeed, they would not have shopped at Target at all during the period of the Target data breach—had Target told them that it lacked adequate computer systems and data security practices to safeguard customers' personal and financial information from theft, and had Target provided them with timely and accurate notice of the Target data breach.

115. Each of the Consumer Plaintiffs suffered actual injury from having their credit or debit card account and personal information compromised and stolen in and as a result of the Target data breach.

116. Each of the Consumer Plaintiffs suffered actual injury and damages in paying money to and purchasing products from Target during the Target data breach that they would not have paid had Target disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Target provided timely and accurate notice of the data breach.

117. Each of the Consumer Plaintiffs suffered actual injury in the form of damages to and diminution in the value of his or her personal and financial information entrusted to Target for the purpose of purchasing its products and that was compromised in and as a result of the Target data breach.

118. Each of the Consumer Plaintiffs was overcharged for purchases made at a Target store using their credit or debit card during the Target data breach in that a portion of the purchase price included the costs of Target providing reasonable and adequate safeguards and data security measures to protect customers' financial and personal data, which Target failed to provide and, as a result, Consumer Plaintiffs did not receive what they paid for and were overcharged.

119. Each of the Consumer Plaintiffs has suffered imminent, certainly impending injury arising from the substantially increased risk of future potential fraud, identity theft and misuse posed by his or her personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Target data breach via sale of Consumer Plaintiffs' and Class members' personal and financial information on the Internet black market.

120. None of the Consumer Plaintiffs who suffered a loss of use of their account funds, or had restrictions placed on their accounts, as a result of the Target data breach was reimbursed

for the loss of access to or restrictions placed upon their accounts and the resulting loss of use of their own funds.

121. Defendant Target Corporation is a Minnesota corporation with its principal place of business located at 1000 Nicollet Mall Avenue, Minneapolis, Minnesota 55403.

IV. STATEMENT OF FACTS

122. Target is the second largest retailer in the United States with 1,797 store locations and annual U.S. sales in 2013 of $71.279 billion. Beginning on or about November 15, 2013 and continuing through December 17, 2013, Target's computer systems were breached by hackers who obtained the financial and personal information of an estimated 110 million Target customers.

123. Target easily could have prevented the data breach from ever occurring. Target failed to take adequate and reasonable measures to ensure its data systems were protected against theft, ignored clear warnings that hackers had breached its systems and failed to take actions that could have stopped the breach in its tracks. Target failed to disclose to Consumer Plaintiffs and members of the Class that its computer systems and security practices were inadequate to reasonably safeguard customers' personal and financial information and failed to immediately and accurately notify its customers of the data breach. As a direct result of Target's conduct, Consumer Plaintiffs and members of the Class were injured.

A. "Kill Chain" Analysis and the Anatomy of the Target Breach

124. The factual background of the Target data breach set forth in the following paragraphs is presented in chronological order and broken into three time periods: (1) the **Pre-Breach**, from January 2013 to November 15, 2013; (2) the **Breach** itself, from November 15, 2013 to December 17, 2013; and (3) the **Post-Breach**, from December 17, 2013 to the present.

In this factual background describing the Target data breach, Consumer Plaintiffs use the intrusion "kill chain" framework, an analytical tool created by Lockheed Martin security researchers in 2011. The kill chain was developed as a response to a new, sophisticated type of hacking called advanced persistent threats ("APTs"), since APTs were easily bypassing traditional static cyber security tools.

125. The kill chain continuously monitors a company's systems for evidence that attackers are trying to gain access to their systems. The purpose of constant vigilance is to level the playing field between the hackers and the companies whose systems they seek to infiltrate.

126. The fundamental premise of kill chain security is that hackers must proceed through seven steps to plan and execute an attack. These steps are called the "kill chain." While the hackers must complete all of these steps to execute a successful attack, the company has to stop the hackers from completing *just one* of these steps to prevent completion of the attack and data loss. Put simply, a company has seven different chances along the kill chain to prevent the attack from occurring. In the following paragraphs, Consumer Plaintiffs identify each link in the kill chain with respect to the Target data breach, explain how the hackers succeeded in moving from one link to the next and describe how Target failed to break the chain–prevent the breach–despite repeated opportunities to do so.

1. Pre-Breach: January 2013 – November 15, 2013

127. In January 2013, the Target security operations center, located in Minneapolis, Minnesota, began the process of updating its computer security systems, including its malware detection software. Target's decision was made at a time when cyber-attacks on U.S. retailers were becoming more and more prevalent, as reflected in numerous reports published on the subject in 2013.

128. Several noteworthy reports published in 2013 put, or should have put, Target on notice of the increase in cyber-attacks on U.S. retailers. For example, the U.S. government and several private research firms distributed industry-wide memos in 2013 on the emergence of new types of malicious computer code targeting retailers.

129. Visa Corporation also issued reports in April and August 2013, alerting Target to attacks using RAM scraper malware, or memory parsing software, which enables cyber criminals to capture encrypted data when it travels through the live memory of a computer. The reports detailed how the attacks were being launched and provided advice on thwarting them.

130. Visa warned Target, "[s]ince January 2013, Visa has seen an increase in network intrusions involving retail merchants," explaining that hackers would "install memory parser malware on the Windows based cash register system in each lane or on Back-of-the-House (BOH) servers to extract full magnetic stipe data." According to this warning, Visa was only aware of the malware impacting the Windows operating system—the exact operating systems Target used—and not any other operating system.

131. To guard against this threat, the Visa warnings instructed Target to, among other things, review its "firewall configuration and ensure only allowed ports, services and IP addresses are communicating with your network"; "segregate the payment processing network from other non-payment processing networks"; "implement hardware-based *point-to-point* encryption"; "perform periodic scans on systems to identify storage of cardholder data and securely delete the data"; and "assign strong passwords to your security solution to prevent application modification." Target failed to implement these measures.

132. Target and other retailers saw a "significant uptick" in malware trying to enter their computer systems throughout 2013.

133. In February 2013, Target hired FireEye, Inc. ("FireEye"), a security software company, to update its computer security systems. FireEye's services included providing Target with malware detection tools, including a team of security specialists whose job was to monitor Target's computers around the clock.

134. From March to May 2013, Target tested FireEye's security software, including its malware detection tools.

135. In June 2013, Target began to roll out its FireEye security software technology throughout its massive IT system. FireEye's security software was installed and functional prior to the date of the Target data breach.

2. Kill Chain 1st Link—Reconnaissance: June 2013 – August 2013

136. Hackers in Eastern Europe, including a hacker who goes by the moniker "Rescator" and was involved in the Target data breach, began probing the computer networks of various major U.S. retailers, including Target. The hackers were searching for loose portals that would allow them access into the retailer's corporate computer systems.

137. The hackers' probing led them to Fazio Mechanical Services ("Fazio"), a Pennsylvania refrigeration and HVAC company.

138. Fazio was a third party vendor to Target; it worked as a heating and air conditioning subcontractor at various Target stores in the U.S. As part of its subcontractor work, Fazio was given limited network credentials by Target, which allowed Fazio virtual access to certain parts of Target's computer network. Target provided the credentials to Fazio to use for electronic billing, contract submission, and project management purposes.

139. To disrupt the reconnaissance step in the kill chain, Target could and should have limited the amount of publicly available vendor information. Hackers were able to gather Target

vendor information by a simple Google search. Target could and should have also shared threat information with its suppliers and vendors and encouraged collaboration within its community of merchants.

3. Kill Chain 2nd Link—Weaponization: September 2013

140. Once the hackers learned that Fazio possessed credentials to Target's computer network, the hackers stole the credentials from Fazio sometime in September 2013, by using a malware called Citadel. The hackers sent the Citadel malware program to Fazio in an email. When Fazio opened the email, Citadel stole all of Fazio's passwords.

141. The theft of the credentials by the hackers was made possible due in part to the grossly inadequate computer security systems in place at Fazio at the time of the theft. Specifically, Fazio's primary method of detecting malicious software – which is what the hackers used to steal the Target credentials – was a free version of a security program called Malwarebytes Anti-Malware ("MBAM"). MBAM is made for individual use and its license expressly prohibits corporate use, which is exactly how Fazio was using it at the time of the attack. Thus, with effectively no malicious software detection program in place at Fazio, the hackers easily stole Fazio's Target credentials.

142. To disrupt the weaponization step in the kill chain, Target could and should have required adequate monitoring and anti-malware software for any vendors with access to Target's computer systems.

143. Armed with Fazio's Target credentials, the hackers began preparing for the next phase of their attack.

144. In or about September 2013, numerous members of Target's security staff raised concerns about what they considered to be vulnerabilities in Target's payment card system. The

vulnerabilities were due to updates being made to Target's cash registers, presumably in conjunction with the rolling out of the FireEye security software. The warnings went unheeded. Target officials ordered no further investigation.

145. On September 20, 2013, Target commissioned an audit, which certified that Target is in compliance with all "payment industry requirements," including the Payment Card Industry Data Security Standards ("PCI DSS"), for protecting credit card data. Consumer Plaintiffs allege that Target failed to comply with all payment industry requirements, including PCI DSS, for protecting credit card data.

146. After the data breach, however, Target admitted in its March 14, 2014 Form 10-K filed with the SEC:

> While an independent third-party assessor found the portion of our network that handles payment card data to be compliant with applicable data security standards in the fall of 2013, we expect the forensic investigator working on behalf of the payment card networks nonetheless to claim that we were not in compliance with those standards at the time of the Data Breach.

4. Data Breach and Kill Chain 3rd Link: November 15, 3013 – December 17, 2013

147. On or about November 15, 2013, the Target data breach began.

148. On November 15, 2013, armed with Fazio's Target credentials, the hackers logged onto Target's computer network. Once logged on, Fazio's credentials give the hackers access to the billing, contract submission, and project management portions of Target's computer network only, and presumably nothing else. Target's computer network, however, was not properly segmented to ensure that its most sensitive parts were walled off from the other parts of the network. The hackers exploited that gaping hole and uploaded their malware into the most sensitive part of Target's computer system – its customer payments and personal data network.

149. The hole that left Target vulnerable and exposed to the hackers is called a "segmentation issue," which occurs where computer systems within a network that should not be connected for security reasons are in fact connected. According to industry experts, there should never be a route between a network for an outside contractor (such as Fazio) and the network for payment data. In Target's case, there was and the hackers found it and exploited it.

150. Once inside Target's customer payments and personal data network, the hackers uploaded their card-stealing malicious software onto a small number of cash registers within Target stores. During this time, the hackers tested their point-of-sale malware to ensure it was working as designed.

151. To disrupt the delivery step in the kill chain, Target could and should have required two-factor authentication for its vendors. Two-factor authentication includes a regular password system (like the one the hackers stole from Fazio) augmented by a second step, such as providing a code sent to the vendor's mobile phone or answering extra security questions (answers to which the hackers did not possess). Target did not do so.

152. On November 30, 2013, the hackers installed their data-stealing malware into a majority of Target's in-store cash registers via remote upload over the Target network. The hackers also began to collect card records from live customer transactions. The way the malware worked was simple: when a customer went to any in-store Target cash register to pay for an item, and swiped his or her card, the malware stepped in and captured the shopper's card number and other sensitive personal information.

5. Kill Chain 4th and 5th Links—Exploitation and Installation: November 30, 2013

153. Also on or about November 30, 2013, the hackers installed exfiltration malware – a program that takes the stolen information and moves it from Target's computer systems to the

hackers' computer systems after several days. FireEye, Target's new security software provider, detected that the hackers were uploading the malware and alerted Target's security team about the suspicious activity. Target's security team took no action.

154. Had Target immediately stepped in once alerted by FireEye to the suspicious activities, the kill chain would have been broken and the hackers' would have been completely foiled and stopped.

155. To disrupt the exploitation step in the kill chain, Target could have and should have blocked the effect of the malware on its servers by following up on the several alerts that were triggered by FireEye at the time of malware delivery. Target could have and should have also avoided the breach by paying greater attention to industry and government intelligence analyses, which included recommendations for reducing the risk of a successful attack. Additionally, Target could and should have taken action to address concerns voiced by its security staff regarding vulnerabilities on the company's cash registers. Target did not take such actions.

156. To disrupt the installation step in the kill chain, Target should have taken two security measures called for in the PCI-DSS 2.1, the version of the PCI-DSS in effect at the time of the breach. First, Target could and should have taken the protective step of eliminating unneeded default accounts, which is what the hackers used to gain access to the most sensitive parts of Target's network. Second, Target could and should have required vendors to more closely monitor the integrity of their critical system files. This requirement would have put Fazio on notice that hackers had stolen its Target credentials. Target did neither.

157. On November 30, 2013, at approximately the same time that FireEye, Target's malware detection system, was spotting suspicious activity on Target's computer network,

Target's antivirus system, Symantec Endpoint Protection ("SEP"), also identified the same type of suspicious behavior. Target again took no action pursuant to SEP's warning, just as it took no action in response to FireEye's warnings. Target's inaction allowed the entirely preventable data breach to continue.

158. On December 2, 2013, Target received the ***exact same*** alert from FireEye that it had received on November 30, 2013. Once again, Target failed to respond to the alert, thereby missing yet another opportunity to prevent the data breach from ever occurring.

6. Kill Chain 6th and 7th Link—Command and Control, Actions on Objectives: December 2-17, 2013

159. After multiple missed opportunities by Target to prevent the data breach, the hackers began the process of actually stealing the card information of Target customers from Target's systems.

160. From December 2-15, 2013, with the malware installed on Target's cash registers, and the extractions software on Target's servers, the hackers collected customers' card information in real time, meaning each time a customer swiped their card at a Target store. The data from each register was then automatically sent to one of three staging points – secret places installed on the *Target computer network* where the hackers temporarily stored the data before sending it offshore. The out-of-place data sat undetected on Target's own network for six days in an attempt to avoid setting off any internal alarms within Target's network. After six days, the data was laundered through a variety of sham computer servers, eventually ending up at its final destination – a server in Russia belonging to the hackers.

161. The hackers repeated this process for almost two weeks completely undisturbed.

162. To disrupt the command and control step in the kill chain, Target could have and should have erected strong firewalls between Target's internal systems and the outside Internet

to help disrupt the hackers' ability to command and control the company's computer network as easily as it did. Target could have and should also have filtered or blocked certain Internet connections commonly used from command and control hacking.

163. To disrupt the actions and objectives step in the kill chain, Target could and should have created a list of approved servers to which Target's network was allowed to upload. Specifically, the list could have dismissed connections between Target's networks and Russian-based Internet servers, which, given that Russia was the end location for the stolen data, and a hot bed of fraudulent hacker activity, would have prevented the breach. Importantly, Target's FireEye software reportedly did detect the data exfiltration malware, yet Target did nothing in response to the report. Again had Target acted on this information, it could have stopped the exfiltration of customers' stolen data.

164. On December 11, 2013, a currently unidentified individual within Target first detected the malware used in the breach, and submitted the malware to VirusTotal, a company that produces reports about suspicious files submitted by users. The submission was attributable to someone within Target because the malware was widely thought to be custom-made specifically for the Target intrusion. Therefore, it stands to reason that the person who found and submitted the malware to VirusTotal must work for Target. Despite being on notice of the malware on this date, Target continued to do nothing and let the breach continue for at least four more days.

165. Information stolen from Target's systems quickly flooded the black market, with the hackers quickly selling the valuable information they had stolen. According to the *New York Times*:

> On Dec. 11, one week after hackers breached Target's systems, Easy Solutions, a company that tracks fraud, noticed a ten to twentyfold

> increase in the number of high-value stolen cards on black market web sites, from nearly every bank and credit union.
>
> The black market for credit card and debit card numbers is highly sophisticated, with numerous card-selling sites that are indistinguishable from a modern-day e-commerce site. Many sell cards in bulk to account for the possibility of cancellations. Some go for as little as a quarter. Corporate cards can sell for as much as $45.
>
> But the security blogger Brian Krebs, who first broke news of the Target security breach on his website, said some Target customers' high-value cards were selling for as much as $100 on exclusive black market sites.

166. Throughout the month of December 2013, the hackers uploaded new stolen cards to a card shop website (an illegal website where stolen credit and debit card information is sold). Some stolen cards were lumped together under the moniker "Tortuga," which was to inform purchasers that the stolen cards were unused, high-quality, and worth their purchase price.

167. On December 20, 2013, an illegal card shop website announced the availability of a new database of stolen credit/debit cards called "Barbarossa," which consisted of more than 330,000 debit and credit cards issued by banks in Europe, Asia, Latin America, and Canada. Brian Krebs, a journalist and cybersecurity expert, reported that "[a]ccording to one large bank in the U.S. that purchased a sampling of cards across several countries – all of the cards in the Barbarossa database also were used at Target during the breach timeframe." The cards for sale in the Barbarossa database varied widely in price from $23.62 per card to as high as $135 per card.

168. On December 12, 2013, the bank JP Morgan Chase alerted some credit card companies that fraudulent charges were showing up on credit cards that were all recently used at Target stores in the U.S.

169. Also on December 12, 2013, the U.S. Justice Department contacted Target about the breach. Rather than immediately taking action to rectify its systems and notify the public,

Target took three days to try and confirm the veracity of the U.S. officials' statements, thereby allowing the data breach to continue for an additional three days.

170. Finally, on December 15, 2013, Target began purging its computer system of the hackers' malware, and after two weeks of uninterrupted data collection (the groundwork for which had been laid weeks before that), Target suspended most of the hackers' ability to collect customer billing and personal information. Target has stated, however, in its SEC Form 10-K dated February 1, 2014, that "[p]ayment card data used in transactions made by 56 additional guests in the period between December 16 and December 17 was stolen prior to our disabling malware on one additional registrar that was disconnected from our system when we completed the initial malware removal on December 15."

171. Target had multiple opportunities to identify and prevent the attack on its data systems, but key personnel at Target remained unaware or unconcerned about what had occurred until days after investigations by the Department of Justice and computer security experts identified the massive breach.

7. Post-Breach: December 17, 2013 -- Present

172. Once informed of the breach on December 12, 2013, Target sat on the information for seven days, rather than immediately notifying the public of the massive breach of millions of credit and debit cards that were already flooding the black market. When Target finally did acknowledge the data breach publicly on December 19, 2013, it was only because someone else had already broken the news.

173. Brian Krebs is credited with "breaking" the news of the Target data breach. Sometime before December 19, 2013, Krebs spoke with a fraud analyst at a major bank who informed Krebs that the bank's team had independently confirmed that Target had been breached

after buying a large number of the bank's card accounts from a black market card site run by the Target hackers.

174. With this information and information from other reliable sources, Krebs broke the Target data breach story on his blog, *Krebs on Security*, on December 18, 2013. Earlier that day, Krebs had left voice messages on Target's public affairs line asking about the data breach. In his voice messages left with Target, Krebs specifically mentioned his conversations with the fraud analyst and that the common spending link on the stolen cards was Target. Target ignored Krebs' requests for comment.

175. On December 19, 2013, seven days after it asserts it learned of the breach,[1] Target publicly disclosed for the first time that its payment card data had been compromised. In a press release, Target confirmed that "customer name, credit or debit card number, and the card's expiration date and CVV" (in other words, the full magnetic stripe data embedded in debit and credit cards that Target was prohibited by law from retaining) of approximately 40 million customers had been stolen.

176. Target posted a notification to customers of the data breach on its corporate website, not on its general consumer website, target.com, the shopping website regularly accessed by consumers, thereby decreasing the likelihood that Target shoppers would read the notification.

177. Target attempted to downplay the significance of the breach to avoid jeopardizing holiday sales, reassuring customers that there was "no indication that debit card PINs were impacted." Indeed, Target claimed that it was "confident that PIN numbers are safe and secure" and thieves could not "visit an ATM with a fraudulent card and withdraw cash." In

[1] It is a separate question as to when Target actually learned of the breach, given the warnings and alerts it received (and chose not to act on) including from its own systems on November 30, 2013 and December 2, 2013.

its December 19, 2013 statement, Target further claimed to "have worked swiftly to resolve the incident" and downplayed the threat to consumers.

178. Target offered a 10% discount on all in-store purchases the weekend before Christmas 2013 in an effort to induce wary customers who were not shopping at Target because of fears associated with the data breach. Despite its efforts, Target experienced tangible damage to customer loyalty and lost sales and revenues resulting from the data breach.

179. Contrary to Target's initial misleading statements, on December 27, 2013 (two days *after* the Christmas holiday), Target admitted that, in fact, "PIN data was removed" from Target's systems.

180. On January 10, 2014, Target announced that the breach was far greater than it originally reported, now admitting that up to 110 million people were affected by the breach. Target stated that in addition to the 40 million customers whose payment card data was compromised, approximately 70 million customer names, mailing addresses, phone numbers and email addresses were also stolen in the data breach. Target admitted that the new subset of victims included customers who may not have shopped at Target during the holiday period previously mentioned in Target's first public press release, thereby suggesting that the data breach may have extended to billing information that Target had stored for a lengthy period of time. Target stated that while there may be some overlap between the two groups (the approximately 40 million customers whose payment card data was compromised and approximately 70 million customers whose personal data was stolen), it did not know the extent of the overlap.

181. In addition to exponentially increasing its estimate of the volume of the breach, Target also disclosed that the nature of the data stolen was much broader, and much worse, than

originally thought. Target admitted that "[i]n addition to the already-known customer names, card numbers, expiration dates and the CVV three-digit security codes that were stolen - the new information included in the breach now includes names, mailing address, phone numbers and email address." Target further conceded that the 110 million customers affected by the breach included customers *who did not even swipe* their debit or credit cards at a Target store in the November to December 2013 period during which Target originally claimed customer data had been compromised, confirming that Target had improperly retained customer data (potentially for many months) that the hackers also extracted as a result of the breach.

182. Targets then-CEO Gregg Steinhafel issued a statement saying: "I know that it is frustrating for our guests to learn that this information was taken, and we are truly sorry they are having to endure this" and on January 12, 2014, in an interview with CNBC, Gregg Steinhafel confirmed that a hacker stole card data by installing malicious software on cash registers used in the checkout lines at Target stores.

183. On January 13, 2014, Target offered one-year of credit monitoring to its customers. Customers were required to request an activation code via email before April 23, 2014 and then register for the offer through the credit monitoring provider before April 30, 2014, after which the offer was no longer available. Target's limited offer of free credit monitoring is inadequate. Credit monitoring services do nothing to prevent credit card fraud. Credit monitoring only informs a consumer of instances of fraudulent opening of new accounts, not fraudulent use of existing credit cards. Agencies of the federal government and privacy experts acknowledge that stolen data may be held for more than a year before being used to commit identify theft and once stolen data has been sold or posted on the Internet, fraudulent use of the stolen data may continue for years.

184. On January 17, 2014, the FBI released a private industry notification warning that the basic code making up the malware used in the Target data breach has been around since at least 2011.

185. On January 21, 2014, "Rescator's" network of black market card stores released for sale a new batch of 2 million cards stolen from Target. "Rescator" called the new batch of cards "Eagle Claw," different from "Tortuga," the original name of card batches released by "Rescator."

186. Despite receiving multiple warnings from government and industry security experts, its own employees, and even its own computer security system, Target took no action to protect its customers' information and personal identifying data. Target's unreasonable data practices and policies have caused Consumer Plaintiffs and Class members to suffer damages as a direct result of Target's misconduct.

187. An investigation by *Bloomberg Businessweek*, citing conversations with "10 former Target employees familiar with the company's data security operation, as well as eight people with specific knowledge of the hack and its aftermath," found, and Consumer Plaintiffs allege, that FireEye's malware detection program worked. But Target "stood by as 40 million credit card numbers—and 70 million addresses, phone numbers, and other pieces of personal information—gushed out of its mainframes." As Bloomberg further stated:

> In testimony before Congress, Target has said that it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that company investigators went back to figure out what happened. What it hasn't publicly revealed: Poring over computer logs, Target found FireEye's alerts from Nov. 30 and more from Dec. 2, when hackers installed yet another version of the malware. Not only should those alarms have been impossible to miss, they went off early enough that the hackers hadn't begun transmitting the stolen card data out of Target's network. Had the company's security team responded when it was supposed to, the theft that has since engulfed Target, touched as many

> as one in three American consumers, and led to an international manhunt for the hackers never would have happened at all.
>
> * * *
>
> On Nov. 30, according to a person who has consulted on Target's investigation but is not authorized to speak on the record, the hackers deployed their custom-made code, triggering a FireEye alert that indicated unfamiliar malware: "malware.binary." Details soon followed, including addresses for the servers where the hackers wanted their stolen data to be sent. As the hackers inserted more versions of the same malware (they may have used as many as five, security researchers say), the security system sent out more alerts, each the most urgent on FireEye's graded scale, says the person who has consulted on Target's probe.
>
> The breach could have been stopped there without human intervention. The system has an option to automatically delete malware as it's detected. But according to two people who audited FireEye's performance after the breach, Target's security team turned that function off.

188. Bloomberg's report was later referenced and substantiated by an investigation, analysis, and report by the United States Senate's Committee on Commerce, Science and Transportation. Utilizing a "Kill Chain analysis" the Senate report concluded as follows:

> This analysis suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach. Key points at which Target apparently failed to detect and stop the attack include, but are not limited to, the following:
>
> - Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor's weak security allowed the attackers to gain a foothold in Target's network.
>
> - Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system.
>
> - Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets.

- Target appears to have failed to respond to multiple warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network.

189. These findings were consistent with other news reports, virtually all of which concluded that the breach of Target's data systems was a result of both inadequate security and a total failure to respond. For example, *The New York Times* reported that Target's security systems were so "astonishingly" open that hackers were able to wander freely throughout Target's computer systems, downloading customer information at will. The same article went on to report that interviews with "people knowledgeable about the investigation, cybersecurity and credit experts" confirmed that Target's "system was particularly vulnerable to attack" and, according to experts, was so "remarkably open" that hackers were able to "wander from system to system, scooping up batches of information."

190. Publically available information indicates the massive scope of the data breach, and Target's cavalier attitude to the sensitive data entrusted to it, was endemic to Target's culture. As profiled in a 2012 article in *The New York Times*:

> *For decades, Target has collected vast amounts of data on every person who regularly walks into one of its stores*. Whenever possible, Target assigns each shopper a unique code — known internally as the Guest ID number — that keeps tabs on everything they buy. "If you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail we've sent you or visit our Web site, we'll record it and link it to your Guest ID," [Target executive Andrew] Pole said. "We want to know everything we can."

191. Indeed, Target's collection, storage and analysis of customer data is so extensive that, as *The New York Times* reported, Target developed a program that used the customer data it collected to predict when a customer might be pregnant in order to direct advertisements for baby products at that customer, and to influence shopping behavior. As reported:

> One Target employee I spoke to provided a hypothetical example. Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There's, say, an 87 percent chance that she's pregnant and that her delivery date is sometime in late August. What's more, because of the data attached to her Guest ID number, Target knows how to trigger Jenny's habits. They know that if she receives a coupon via e-mail, it will most likely cue her to buy online. *They know that if she receives an ad in the mail on Friday, she frequently uses it on a weekend trip to the store.*

192. Target has also admitted that it has *kept sensitive customer financial data for 60 to 80 days*. That fact was confirmed by John Deters, a Target engineering consultant who testified on behalf of Target in litigation alleging that Target violated provisions of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") by improperly printing credit and debit account information, including the full account number and card expiration date, on credit and debit transaction receipts. As Deters testified, "Target retain[s] the full account number" and "then store[s] that information regarding the transaction, including the account numbers of the—of the credit card or debit card and the expiration date and the cardholder's name, in its computer system." As explained by John Kindervag, an analyst from Forrester Research and a leading security expert, "[Target] is a breach that should've never happened . . . *The fact that three-digit CVV security codes were compromised shows they were being stored . . . .*" (Emphasis added.)

193. Target's public acknowledgement that it was failing to adhere to industry standards regarding the retention and use of credit and debit card information not only confirms that Target failed to take measures that led to its vulnerability, but also that those failures may have put hackers on notice that one of the largest retailers in the world was carefully cataloging and keeping the credit and debit card information of all of its customers.

194. On March 5, 2014, Beth Jacob, Target's Chief Information Officer and the highest-ranking technology executive at Target, resigned in the aftermath of the Target data

breach and revelations about Target's data collection and security practices. On May 5, 2014, CEO Gregg Steinhafel also resigned.

B. Target was well aware of its obligations to safeguard customer data

195. Target was at all times fully aware of its obligations under the law and various standards and regulations to protect data entrusted to it by consumers.

196. Since August 1, 2007, the Minnesota Legislature has set strict time limitations on the retention of credit and debit card information by businesses:

> No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

Minn. Stat. § 325E.64 (known as the Minnesota's Plastic Card Security Act).

197. Target retained Consumer Plaintiffs' and Class members' "card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data" beyond these statutory time limits ("subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction"). The above facts concerning the extended period of the breach indicate that Target routinely holds such customer data longer than allowed under Minn. Stat. § 325E.64. Target's unlawful retention of such data contributed to and allowed the data breach to occur.

198. The Payment Card Industry Data Security Standards ("PCI DSS") list twelve information security requirements promulgated by the Payment Card Industry Security Standards Council. These industry requirements apply to all organizations and environments where

cardholder data is stored, processed, or transmitted and require merchants, including Target, to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies. The PCI DSS prohibited Target from retaining certain customer data. Specifically, the PCI DSS 2.0 requires merchants to adhere to the following rules:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
- Protect stored cardholder data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel

199. Additionally, financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants such as Target must take to ensure that valuable transactional data is secure and protected. The debit and credit card companies issue regulations ("Card Operating Regulations") that bind Target as a condition of its contract with its acquiring bank. The Card Operating Regulations prohibit Target and other merchants from disclosing any card holder account numbers, personal information, magnetic stripe information or transaction information to third parties (other than the merchant's agent, the acquiring bank, or the acquiring bank's agents). The Card Operating Regulations further require Target to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

200. Despite Target's awareness of its data protection obligations, Target's treatment of the financial account and personally identifying information entrusted to it by its customers fell far short of satisfying Target's legal duties and obligations. Target failed to ensure that access to its data systems was reasonably safeguarded. Target failed to acknowledge and act upon numerous warning signs and properly utilize its own security systems that were put in place to detect and deter this exact type of attack.

C. Target had numerous additional warnings in the years leading up to the Target security breach

201. At the time of the breach, Target had specific notice of the potential attacks that could occur on its systems, and of the potential risks posed to Target and its customers, including Consumer Plaintiffs and Class members, if it failed to adequately protect its systems.

202. For example, and in addition to the reports and warnings set forth in the above paragraphs 127- 131, as early as 2005, a notorious IT systems hacker, Albert Gonzalez, masterminded and implemented one of the largest coordinated data breaches in history, ultimately compromising more than 170 million credit and debit card accounts by infecting retailers' point of sale ("POS") terminals with malicious software (also known as malware) which transmitted, unencrypted, the financial data being processed by the POS machine to Gonzalez and his accomplices. In the end, Gonzalez and his cohorts were able to walk off with vast amounts of customer data from various retailers, *including customer data possessed by Target*. In fact, the Gonzalez data breach led to passage of the Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64.

203. In May 2010, weaknesses in Target's POS systems were again exploited by hackers. As reported by the online retailer security newsletter, FierceRetailIT, Target had somehow "overlooked security holes" in its POS systems that enabled customers to use funds from other shoppers' gift cards. The security expert who identified these "holes"—which included printing the full account number ("PAN" or "Primary Account Number") in the gift card's barcode—described them as fundamental security failures. According to the expert, "You never use the PAN on the handset. Never, never."

204. Later, on April 5, 2011, Target informed its "customers that their names and email addresses had been exposed in a massive online data breach" when a computer hacker penetrated the customer email databases in which Target retained customers' personal information.

205. Indeed, the vulnerability of corporate point-of-sale ("POS") systems was made known to Target years before the Target data breach.

206. On August 27, 2007, Dr. Neal Krawetz of Hacker Factor Solutions publicly disclosed a white paper titled "Point-Of-Sale Vulnerabilities" (the "White Paper"). The White Paper abstract described its content as follows:

> Point-of-Sale (POS) systems provide the initial interface for credit card transactions. While the communications between POS systems have been hardened through the use of cryptography and a variety of authentication techniques, the devices themselves provide virtually no security. Few POS systems implement best practices for handling sensitive information, such as the Visa standards for credit card management. This document describes common risks to credit card users due to POS systems.

207. The White Paper then provided a detailed description of the typical POS system and its components, including "5.2.2 Lax security processes" and "5.3 Security up for Auction." The White Paper described POS "Branch Servers" and how their vulnerability could result in the compromise of millions of credit card accounts.

208. Presciently, the 2007 White Paper used Target as an example of the potential ramifications of a POS data breach at a major retailer. It estimated that as many as 58 million card accounts could be compromised if Target's POS system was compromised. For a paper written over six years before the Target data breach at issue here, Dr. Krawetz' estimate using assumed transaction frequency and data storage times is remarkably close.

209. In his conclusion for the White Paper, Dr. Krawetz specifically notes:

> Point-of-sale terminals and branch servers store credit card information in ways that are no longer secure enough. These vulnerabilities are not limited to any single POS vendor; they pose a fundamental hole in the entire POS market. It seems that nearly every POS provider is vulnerable, including Verifone, Fujitsu Transaction Solutions, Retalix, Hypercom, Autostar, Innovax, IDA, JPMA, NCR, StoreNext, IBM, and Systech. Similarly, these vulnerabilities impact all retailers that use these systems, including (but not limited to) OfficeMax, BestBuy, Circuit City, Target, Wal-Mart, REI, Staples, Nordstrom, and Petco. The amount of vulnerability varies between retailers and their implementations. But in general, if a credit card is not required to return a product, or the product

> can be returned at any store, then the retailer likely has a serious vulnerability.

210. Dr. Krawetz summarizes the vulnerable aspects of the POS architecture, including Branch Servers and closes:

> Even though other sightings have occasionally surfaced, the February 9th [2006] announcement showed the first big vendor being publicly hit with this problem. This compromise was not the first, it is unlikely to be the last, and it certainly will not be the biggest. **It is only a matter of time before a national branch server at a large retailer is compromised.** (Emphasis added.)

211. On or about August 7, 2007, a Target employee responsible for Target's POS system acknowledged receipt of the White Paper and requested permission to provide it to other Target employees. The Target employee described Dr. Krawetz suggestions as "good ideas."

212. Dr. Krawetz's website logs the web domains that download copies of his documents. A domain registered to Target Corporation downloaded 17 copies of the White Paper between August 2007 and May 2013. Search terms that led to downloads of the White Paper to the Target domain as late as May 2013, included "POS vulnerability."

213. On information and belief, Target did not implement the suggestions in the White Paper.

D. Consumers' personal and financial information is valuable

214. The personal and financial information of consumers, including Consumer Plaintiffs and Class members, is valuable.

215. The FTC warns consumers to pay particular attention to how they keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. As the FTC notes, "[t]hat's what thieves use most often to commit fraud or identity theft."

216. The information stolen from Target, including Consumer Plaintiffs' and Class members' financial and personal information, is extremely valuable to thieves. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."

217. Personal and financial information such as that stolen in the Target data breach is highly coveted by and a frequent target of hackers. Legitimate organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use biographical data to perpetuate more and larger thefts.

218. As noted by Brian Krebs on his blog, data stolen in the Target data breach, including "track data," enables crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe. The thieves use the credit card information to create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards. Additionally, the thieves could reproduce stolen debit cards and use them to withdraw cash from ATMs.

219. The ramifications of Target's failure to keep Plaintiffs' and Class Members' personal and financial information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes.

220. According to experts, one out of four data breach notification recipients became a victim of identity fraud.

221. Identity thieves can use personal information such as that pertaining to Consumer Plaintiffs and the Class, which Target failed to keep secure, to perpetuate a variety of crimes that harm the victims. For instance, identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

222. In addition, identity thieves may get medical services using consumers' lost information or commit any number of other frauds, such as obtaining a job, procuring housing or even giving false information to police during an arrest.

223. As previously noted, a cyber black market exists in which criminals openly post and sell stolen credit card numbers, Social Security numbers and other personal information on a number of Internet websites.

224. The personal and financial information that Target failed to adequately protect and that was stolen in the Target data breach, including Consumer Plaintiffs' and Class members' identifying information, is "as good as gold" to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts or clone ATM, debit or credit cards.

225. As previously explained, Consumer Plaintiffs' and Class members' personal and financial information stolen from Target flooded the underground black market with batches of fake credit cards selling, for example, from $20 to $100 per card. The online black market also

provided thieves with the zip code and location of the Target store where the information was stolen, allowing thieves to make same-state purchases and avoid any blocks from banks suspecting fraud.

226. The Senate Committee Report on the Target data breach states:

> Thieves were able to sell information from these cards via online black market forums known as "card shops." Those purchasing information can then create and use counterfeit cards with the track data and PIN stolen from credit and debit card magnetic stripes. Fraudsters often use these cards to purchase high-dollar items and fence them for cash. Or, rather and if PIN numbers are available, a thief can extract a victim's money directly from an ATM.

227. *Bloomberg Businessweek* further reported on the availability of specific-location stolen credit cards available on the internet black-market:

> For Minnetonka, about 12 miles from Target's headquarters with a population of 51,000, there are 7,000 cards for sale. For another Minneapolis suburb, Plymouth, population 73,000, there are 5,335 cards available. Fayetteville, Ark.: 3,685. Torrington, Conn.: 5,115. The cards run from $6 a piece for a prepaid gift card to almost $200 for an American Express Platinum, and Rescator accepts payments in Bitcoin and Western Union (WU). The return period – just in case some of the cards don't work – is six hours, according to the site's Replace Policy page, which is printed in Russian and English for better customer service. Long before six hours elapse, thieves can have the stash of stolen numbers printed on counterfeit cards and charge up a storm of purchases at stores or online, often in the form of gift cards that are easily transformed into cash. Eventually a bank catches wind of the fraud and freezes the card. For the thief, it's on to the next one.

E. Target failed to disclose material facts

228. Target failed to inform or disclose to the public, including Consumer Plaintiffs and members of the Class, material facts that would have influenced the purchasing decisions of Consumer Plaintiffs and Class members.

229. Target failed to disclose to the public, including Consumer Plaintiffs and members of the Class, that its computer systems and security practices were inadequate to safeguard customers' financial account and personal identifying information against theft.

230. Target failed to disclose and provide timely and accurate notice of the data breach to the public, including Consumer Plaintiffs and members of the Class.

231. Consumer Plaintiffs and members of the Class believed that Target would maintain their personal and financial information in a reasonably secure manner and they provided their personal and financial information to Target on that basis for the purpose of purchasing goods from Target.

232. Had Target disclosed to Consumer Plaintiffs and members of the Class that Target did not have adequate computer systems and security practices to secure customers' account and personal information, Consumer Plaintiffs and members of the Class would not have made purchases at Target using their credit or debit cards and would not have purchased goods at Target at all.

233. Target continued to accept credit and debit card payments from Consumer Plaintiffs and Class members after Target knew or should have known that its systems were being or had been breached, without disclosing the breach in a timely and accurate manner and without unreasonable delay.

234. Target recognizes that its customers' personal and financial information is highly sensitive and must be protected.

235. For years, Target has publicly stated in Target's Privacy Policy website that it protects customers' personal information. For example, in its May 8, 2006 posting of Target's Privacy Policy, Target stated the following:

> **Security Methods**
>
> **Our Commitment to Data Security**
>
> We have appropriate physical, electronics and procedural security safeguards to protect and secure the information we collect.
>
> **Secure Sockets Layering (SSL)**
>
> Our website uses Secure Sockets Layering (SSL) to encrypt your personal credit information, including your credit card number, before it travels over the Internet. Technology is the industry standard for secure online transactions. Because we use SL, placing an order online at our website is just as safe as giving your credit card number over the phone.
>
> **Safe Shopping Guarantee**
>
> Our security measures are designed to prevent anyone from stealing and using your credit card number.

236. Over the years Target made various amendments to its Target Privacy Policy but continued to represent that it provides safeguards to protect and secure the information it collects. In the version of its Privacy Policy as it appeared on Targets' website on October 3, 2013 and November 7, 2013, Target stated:

> **How is Your Personal Information Protected?**
>
> **Security Methods**
>
> We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as credit or debit card numbers, we use industry standard methods to protect that information. However, no e-commerce solution, website, database or system is completely secure or "hacker proof." You are responsible for taking reasonable steps to protect your personal information against unauthorized disclosure or misuse.

237. As previously alleged, contrary to its representations, Target failed to provide reasonable and adequate data security, including pursuant to and in compliance with industry standards and applicable law.

238. Target has acknowledged the substantial economic harm caused by the data breach. In its February 1, 2014 Form 10-K filed with the SEC, Target states that:

> We believe the Data Breach adversely affected our fourth quarter U.S. Segment sales. Prior to our December 19, 2013 announcement of the data breach, U.S. Segment fourth quarter comparable sales were positive, followed by meaningfully negative comparable sales results following the announcement.

239. Target has furthered reported that its net earnings for the fourth quarter of 2013, which includes the time period of the data breach, declined to 46%. In its SEC Form 8-K dated February 26, 2014, Target states:

> In fourth quarter 2013, sales decreased 6.6 percent to $20.9 billion from $22.4 billion last year, reflecting the impact of an additional accounting week in 2012 and a 2.5percent decrease in comparable sales, partially offset by the contribution from new stores.

V. CLASS ALLEGATIONS

240. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiffs bring their claims that Target violated state consumer statues (Count I) on behalf of separate statewide classes in and under the respective consumer laws of each state of the United States and the District of Columbia as set forth in Count I. These classes are defined as follows:

> **Statewide Consumer Law Classes**:
>
> All residents of [name of State or District of Columbia] whose credit or debit card information and/or whose personal information was compromised as a result of the data breach first disclosed by Target on December 19, 2013.

241. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiffs bring their claims that Target violated state data breach statutes (Count II) on behalf of separate statewide classes in and under the respective data breach statutes of the States of Alaska, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky,

Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia. These classes are defined as follows:

> **Statewide Data Breach Statute Classes**:
>
> All residents of [name of above State or District of Columbia] whose credit or debit card information and/or whose personal information was compromised as a result of the data breach first disclosed by Target on December 19, 2013.

242. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiffs bring their separate claims for negligence (Count III), breach of implied contract (Count IV), bailment Count (VI) and unjust enrichment (Count VII) on behalf of the respective statewide classes in and under the laws of each respective State of the United States and the District of Columbia as set forth in Counts III, IV, VI and VII. These classes for each of the foregoing claims are defined as follows:

> **Statewide [Negligence, Breach of Implied Contract, Bailment or Unjust Enrichment] Class**:
>
> All residents of [name of State or District of Columbia] whose credit or debit card information and/or whose personal and financial information was compromised as a result of the data breach first disclosed by Target on December 19, 2013.

243. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiffs bring their REDcard debit card breach of contract claim (Count V) under South Dakota law as set forth in Count V and on behalf of a nationwide class defined as follows:

> **Nationwide Target REDcard Class**:
>
> All residents of the United States whose Target REDcard debit card information and/or whose personal information was compromised as a result of the data breach first disclosed by Target on December 19, 2013.

244. Excluded from each of the above Classes are Target Corporation, including any entity in which Target has a controlling interest, is a parent or subsidiary, or which is controlled by Target, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Target. Also excluded are the judges and court personnel in this case and any members of their immediate families.

245. Certification of Consumer Plaintiffs' claims for class-wide treatment is appropriate because Consumer Plaintiffs can prove the elements of their claims on a class-wide basis using the same exclusive and common evidence as would be used to prove those elements in individual actions alleging the same claims.

246. All members of the purposed Classes are readily ascertainable. Target has access to addresses and other contact information for millions of members of the Classes, which can be used for providing notice to many Class members.

247. **Numerosity**. Each Class is so numerous that joinder of all members would be impracticable. While the precise number of Class members has not yet been determined, Target has admitted that 40 million credit and debit card accounts and PINs were stolen and as many as 70 million persons had their personal information compromised in the Target data breach. While the number of REDcard debit card Class members is not known to Consumer Plaintiffs, Target indicates in its 2013 Form 10-K filed with the SEC that total REDcard sales for 2013 constituted 19.3% of Target's 2013 annual sales of $71.279 billion.

248. **Commonality**. Questions of law and fact common to all Class members exist and predominate over any questions affecting only individual Class members, including, but not limited to the following:

a. whether Target engaged in the wrongful conduct alleged herein;

b. whether Target's conduct constituted unfair methods of competition and/or was deceptive, unfair, unconscionable and/or unlawful;

c. whether Target's conduct was likely to deceive a reasonable person;

d. whether Target owed a duty to Consumer Plaintiffs and members of the Class to adequately protect their personal and financial information and to provide timely and accurate notice of the Target data breach to Consumer Plaintiffs and members of the Class;

e. whether Target breached its duties to protect the personal and financial information of Consumer Plaintiffs and members of the Class by failing to provide adequate data security and whether Target breached its duty to provide timely and accurate notice to Consumer Plaintiffs and members of the Class;

f. whether Target knew or should have known that its computer systems were vulnerable to attack;

g. whether Target's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of millions of consumers' personal and financial data;

h. whether Target improperly retained credit and/or debit sales transaction data beyond the period of time permitted by law, including under Minn. Stat. § 325E.64;

i. whether Target unlawfully failed to inform Consumer Plaintiffs and members of the Class that it did not maintain computers and security practices adequate to reasonably safeguard customers' financial and personal data and whether Target failed to inform Consumer Plaintiffs and members of the Class of the data breach in a timely and accurate manner;

j. whether Consumer Plaintiffs and members of the Class suffered injury, including ascertainable losses, as a result of Target's conduct (or failure to act);

k. whether Consumer Plaintiffs and members and Class are entitled to recover actual damages and/or statutory damages;

l. whether Consumer Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement and/or other equitable relief.

249. **Typicality**. Consumer Plaintiffs' claims are typical of the claims of the Class. Consumer Plaintiffs and all Class members were injured through Target's uniform misconduct described above and assert the same claims for relief. The same events and conduct that give rise to Consumer Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because each Consumer Plaintiff and Class member is a person that has suffered harm as a direct result of the same conduct (and omissions of material facts) engaged in by Target and resulting in the Target data breach.

250. **Adequacy**. Consumer Plaintiffs and their counsel will fairly and adequately represent the interests of the Class members. Consumer Plaintiffs have no interest antagonistic

to, or in conflict with, the interests of the Class members. Consumer Plaintiffs' lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation.

251. **Superiority**. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Consumer Plaintiffs and the Class members. Consumer Plaintiffs and the Class members have been harmed by Target's wrongful actions and inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Target's wrongful actions and inaction.

252. A class action is an appropriate method for the fair and efficient adjudication of this controversy. There is no special interest in the members of the Class individually controlling the prosecution of separate actions. The loss of money and other harm sustained by many individual Class members will not be large enough to justify individual actions, especially in proportion to the significant costs and expenses necessary to prosecute this action. The expense and burden of individual litigation makes it impossible for many members of the Class individually to address the wrongs done to them. Class treatment will permit the adjudication of claims of Class members who could not afford individually to litigate their claims against Target. Class treatment will permit a large number of similarly situated persons to prosecute their common claims in a single form simultaneously, efficiently and without duplication of effort and expense that numerous individual actions would entail. No difficulties are likely to be encountered in the management of this class action that would preclude its maintenance as a class action, and no superior alternative exists for the fair and efficient adjudication of this controversy. Furthermore, Target transacts substantial business in and perpetuated its unlawful

conduct from Minnesota. Target will not be prejudiced or inconvenienced by the maintenance of this class action in this forum.

253. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(3). The above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

254. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Target has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

255. The expense and burden of litigation will substantially impair the ability of Consumer Plaintiffs and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Target will retain the benefits of its wrongdoing despite its serious violations of the law.

VI. COUNTS

COUNT I

VIOLATIONS OF STATE CONSUMER LAWS (ON BEHALF OF CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE CONSUMER LAW CLASSES)

256. Consumer Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1-254, as if fully set forth herein.

257. Consumer Plaintiffs and members of the statewide Consumer Law Class ("Class" as used in this Count I) are consumers who used their credit or debit cards to purchase products from Target primarily for personal, family or household purposes.

258. Target engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Consumer Plaintiffs and members of the Class.

259. Target is engaged in, and its acts and omissions affect, trade and commerce. Target's acts, practices and omissions were done in the course of Target's business of marketing, offering for sale and selling goods and services throughout the United States, including in Minnesota.

260. Target's conduct as alleged in this Complaint, including without limitation, Target's failure to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information, Target's failure to disclose the material fact that Target's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, Target's failure to disclose in a timely and accurate manner to Consumer Plaintiffs and members of the Class the material fact of the Target data security breach, and Target's continued acceptance of Consumer Plaintiffs' and Class members' credit and debit card payments for purchases at Target after Target knew or should have known of the data breach and before it purged its systems of the hackers' malware, constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices.

261. By engaging in such conduct and omissions of material facts, Target has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another", and/or "engaging in any other conduct which similarly creates a likelihood of confusion or of

misunderstanding"; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

262. The damages, ascertainable losses and injuries, including to their money or property, suffered by Consumer Plaintiffs and members of the Class as a direct result of Target's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth in this Complaint include, without limitation: a) unauthorized charges on their debit and credit card accounts; b) theft of their personal and financial information; c) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; d) loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations; e) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Target data breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Target data breach in the weeks leading up to and beyond the end-of-year holiday season; f) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and being already misused via the sale of consumers' information on the Internet card black market; g) damages to and diminution in value of their personal and financial information

entrusted to Target for the purpose of purchasing products from Target and with the understanding that Target would safeguard their data against theft and not allow access and misuse of their data by others; h) money paid for products purchased at Target stores during the period of the Target breach in that Consumer Plaintiffs and Class members would not have shopped at Target had Target disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Target provided timely and accurate notice of the Target data breach; (i) overpayments made to Target for products purchased during the Target data breach in that a portion of the price for such products paid by Consumer Plaintiffs and the Class to Target was for the costs of Target providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Target failed to do and, as a result, Consumer Plaintiffs and members of the Class did not receive what they paid for and were overcharged by Target; and (j) the continued risk to their personal information, which remains in the possession of Target and which is subject to further breaches so long as Target fails to undertake appropriate and adequate measures to protect data in its possession.

263. Target's conduct described in this Complaint, including without limitation, Target's failure to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information, Target's failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect customers' personal and financial information, Target's failure to provide timely and accurate notice to Consumer Plaintiffs and Class members of the material fact of the Target data breach, and Target's continued acceptance of Consumer Plaintiffs' and Class members' credit and debit card payments for purchases at Target after Target knew or should have known of the data breach and

before it purged its systems of the hackers' malware, constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq*.;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq*.;

d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*

e. The Colorado Consumer Protection Act, Col. Rev. Stat. Ann. §§ 6-1-105(1)(b), (c), (e) and (g), *et seq.*;

f. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq*.;

g. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6, § 2532(5) and (7), *et seq*., and the Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, *et seq*.;

h. The District of Columbia Consumer Protection Act, D.C. Code §§ 28-3904(a), (d), (e), (f) and (r), *et seq.*;

i. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq*.;

j. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq.*;

k. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq.*; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq.*;

l. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;

m. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*, and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Stat. § 510/2(a)(5), (7) and (12), *et seq.*;

n. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq.*;

o. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq.*, Consumer Plaintiffs have obtained the approval of the Iowa Attorney General for filing this class action lawsuit as provided under I.C.A § 714H.7;

p. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq.*;

q. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), *et seq.*;

r. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq.*;

s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;

t. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§1212(1)(E) and (G), *et seq.*, and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq.*;

u. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq*;

v. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e), (s) and (cc), *et seq.*;

w. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), *et seq*., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat.§ 8.31, subd. 3(a);

x. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq*.;

y. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq*;

z. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq*.;

aa. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq*.;

bb. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq*.;

cc. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

dd. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq.*;

ee. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;

ff. New York Business Law, N.Y. Gen. Bus. Law § 349(a);

gg. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq.*;

hh. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq.*;

ii. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq.* Pursuant to Ohio Rev. Code Ann. § 1345.09(B), Defendant's alleged acts must have been previously declared to be deceptive or unconscionable under Ohio Rev. Code Ann. §§ 1345.02 or 1345.03. As alleged herein, Target omitted material disclosures that it did not have adequate security to safeguard consumers' financial and personal data; did not timely notify consumers of the data breach; and did not timely act when notified of suspicious activity on its computer network. Ohio courts have previously declared such actions to be deceptive or unconscionable under §§ 1345.02 or 1345.03. *See, e.g.*, *Arales v. Furs by Weiss, Inc.*, No. 81603, 2003 WL 21469131, at *1-4 (Ohio Ct. App. June 26, 2003) (upholding jury determination that retailer's omission to consumer was unfair or deceptive under § 1345.02);

Lump v. Best Door & Window, Inc., Nos. 8-01-09, 8-01-10, 2002 WL 462863, at *4-*5 (Ohio Ct. App. Mar. 27, 2002) (a company's failure to perform obligations to consumers in a timely manner is a deceptive act or unconscionable practice in violation of §§ 1345.02 or 1345.03); *id.* at *5 (a supplier in connection with a consumer transaction who consistently maintains a pattern of inefficiency, incompetency, or continually stalls and evades his legal obligations to consumers, commits an unconscionable act and practice in violation of § 1345.03; *id.* at *10-11 (Walters, J., concurring) ("it is clear that an omission may constitute a deceptive act or practice under" Ohio Rev. Code Ann. § 1345.02); *Baker v. Tri-County Harley Davidson, Inc.*, No. CA98-12-250, 1999 WL 1037262, at *2 (Ohio Ct. App. Nov. 15, 1999) (finding that courts have determined untimeliness "to be a deceptive or unconscionable practice"); *Miner v. Jayco, Inc.*, No. F-99-001, 1999 WL 651945, at *7-8 (Ohio Ct. App. Aug. 27, 1999) ("a supplier in connection with a consumer transaction who consistently maintains a pattern of inefficiency, incompetency, or continually stalls and evades his legal obligations to consumers, commits an unconscionable act and practice in violation of" § 1345.03); *Crye v. Smolak*, 674 N.E.2d 779, 783 (Ohio Ct. App. Apr. 23, 1996) ("untimeliness had been determined to be a deceptive act or unconscionable practice, violating R.C. 1345.02 or 1345.03, by various courts of this state"); *Daniels v. True*, 547 N.E.2d 425, 426-27 (Ohio Misc. 2d Dec. 9, 1988) (same as *Miner*); *Brown v. Lyons*, 332 N.E.2d 380, 386 (Ohio Misc. Nov. 12, 1974) (same).

jj. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5), (7) and (20), *et seq.*; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq*;

kk. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq.*;

ll. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;

mm. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq*;

nn. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*;

oo. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq.*;

pp. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a) and (b)(5) and (7);

qq. The Texas Deceptive Trade Practices- Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq.*;

rr. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);

ss. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq.*;

tt. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*;

uu. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq*.;

vv. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.;

ww. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et seq*.; and

xx. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq*.

264. Consumer Plaintiffs bring this action on behalf of themselves and all similarly situated persons in the proposed separate statewide Consumer Law Classes for the relief requested and for the public benefit in order to promote the public interests in the provision of truthful, non-deceptive information to allow consumers to make informed purchasing decisions and to protect Consumer Plaintiffs and Class members and the public from Target's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful practices. Target's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large, including causing injury and ascertainable losses of money or property to up to 110 million persons across the United States.

265. Prior to the filing of this Complaint, counsel for Consumer Plaintiffs and the statewide Consumer Law Classes provided Target with written pre-suit demands under state consumer laws providing for such demands, including Ala. Code § 8-19-10(e), Alaska Stat. Ann. § 45.50.535(b), Cal. Civ. Code § 1782(a), Ga. Code Ann. § 10-1-399(b), Ind. Code § 24-5-0.5-5(a), Me. Rev. Stat. Ann. Tit. 5, § 213(1-A), Mass. Gen. Laws Ann. Ch. 93A § 9(3), Tex. Bus. & Com. Code Ann. § 17.505(a) and W.Va. Code § 46A-6-106(b). Additionally, Target has long

had notice of Consumer Plaintiffs' allegations, claims and demands including from the filing of numerous actions by various consumer plaintiffs against Target arising from the Target data breach, the first of which were filed on December 19, 2013.

266. Consumer Plaintiffs have provided notice of this action and a copy of this Complaint to the appropriate Attorneys General pursuant to state consumer laws providing for such notice, including Conn. Gen. Stat. § 42-110g(c), 815 Ill. Stat. § 505/6, Kan. Stat. § 50-634(g), La. Rev. Stat. Ann. § 51:1409(B), N.J. Stat. Ann. § 56:8-20, Ore. Rev. Stat. Ann. § 646.638(s) and Wash. Rev. Code § 19.86.095.

COUNT II

VIOLATIONS OF STATE DATA BREACH STATUTES
(ON BEHALF OF CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE DATA BREACH STATUTE CLASSES)

267. Consumer Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs 1-254, as if fully set forth herein.

268. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedient time possible and without unreasonable delay.

269. The Target data breach constituted a breach of the security system of Target within the meaning of the below state data breach statutes and the data breached was protected and covered by the below data breach statutes.

270. Consumer Plaintiffs' and Class members' names, credit and debit card numbers, card expiration dates, CVVs addresses, phone numbers and email addresses constitute personal information under and subject to the below state data breach statutes.

271. Target unreasonably delayed in informing the public, including Consumer Plaintiffs and members of the statewide Data Breach Statute Classes ("Class," as used in this Count II), about the breach of security of Consumer Plaintiffs' and Class members' confidential and non-public personal information after Target knew or should have known that the data breach had occurred.

272. When the Target data breach began on or about November 15, 2013, upon the hackers logging onto Target's computer network, gaining access first through the billing, contract submission and project management portions of Target's computer network, then uploading their malware onto the most sensitive part of Target's computer system (its customers' payments and personal data network), and then proceeding to upload their card-stealing malicious software into cash registers within Target stores—Target did not disclose or notify the public of the data breach.

273. On November 30, 2013, when FireEye, Target's new security software provider, spotted the hackers while they were uploading the malware and alerted Target's security team about the suspicious activity, Target took no action and did not disclose or notify the public of the data breach.

274. On November 30, 2013, when Target's antivirus system, Symantec End Point Protection, identified the same type of suspicious behavior, Target took no action and did not disclose or notify the public of the data breach.

275. On December 2, 2013, when Target received exactly the same alert from FireEye that it had received on November 30, 2013, Target again failed to respond and did not disclose or notify the public of the data breach.

276. From December 2-15, 2013, when the hackers collected customers' card information each time a customer swiped his or her card at a Target store and then sent the data to one of three staging points within Target's own computer network—and for six days before the hackers sent the data outside of Target's systems offshore—Target took no action and did not disclose or notify the public of the data breach.

277. On December 11, 2013, when an unidentified individual within Target detected the malware used in the breach and submitted it to VirusTotal, Target continued to do nothing and did not disclose or notify the public of the data breach.

278. On December 12, 2013, after the U.S. Justice Department contacted Target to alert it to the breach, Target did not disclose or notify the public of the breach but rather scrutinized the Justice Department's information for three days, during which the data breach continued.

279. On December 15, 2013, when Target began purging its computer system of the hackers' malware, Target did not disclose or provide notice to the public of the data breach.

280. Only after Brian Krebs broke the Target data breach story on December 18, 2013 did Target first disclose, on December 19, 2013, that its payment card data had been compromised.

281. As set forth in greater detail above, Target initially attempted to downplay the significance of the breach to preserve its holiday sales, by reassuring customers that there was "no indication that debit card PINs were impacted," asserting its confidence that "PIN numbers

are safe and secure" and attempting to lure customers back to its stores by offering a 10% discount during the remaining holiday shopping days. A week later, on December 27, 2013, after the Christmas holiday ended, Target admitted that "PIN data was removed" from Target's systems. And on January 10, 2014, Target disclosed that up to 110 million people were affected by the breach and that in addition to customer names, card numbers, expiration dates and the CVV three digit codes that were stolen, additional information stolen in the breach included names, mailing addresses, phone numbers and email addresses.

282. Target failed to disclose to Consumer Plaintiffs and Class members without unreasonable delay and in the most expedient time possible, the breach of security of Consumer Plaintiffs' and Class members' personal and financial information when Target knew or reasonably believed such information had been compromised.

283. On information and belief, no law enforcement agency instructed Target that notification to Consumer Plaintiffs and Class members would impede investigation.

284. Consumer Plaintiffs and members of the Class suffered harm directly resulting from Target's failure to provide and the delay in providing Consumer Plaintiffs and Class members with timely and accurate notice as required by the below state data breach statutes. Consumer Plaintiffs suffered the damages alleged above as a direct result of Target's delay in providing timely and accurate notice of the data breach.

285. Had Target provided timely and accurate notice of the Target data breach, Consumer Plaintiffs and Class members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Target in providing notice. Consumer Plaintiffs and Class members could have avoided making credit or debit card purchases at Target stores, could have avoided shopping at Target stores at all, and

could have contacted their banks to cancel their cards, or could otherwise have tried to avoid the harm caused by Target's delay in providing timely and accurate notice.

286. Target's failure to provide timely and accurate notice of the Target data breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Ark. Code Ann. § 4-110-105(a), *et seq.*;

c. Cal. Civ. Code § 1798.83(a), *et seq.*;

d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;

f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

g. D.C. Code § 28-3852(a), *et seq.*;

h. Fla. Stat. Ann. § 501.171(4), *et seq.*;

i. Ga. Code Ann. § 10-1-912(a), *et seq.*;

j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

k. Idaho Code Ann. § 28-51-105(1), *et seq.*;

l. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

m. Iowa Code Ann. § 715C.2(1), *et seq.*;

n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;

s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;

u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

dd. R.I. Gen. Laws Ann. § 11-49.2-3(a), *et seq.*;

ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;

ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;

hh. Utah Code Ann. § 13-44-202(1), *et seq.*;

ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq*.

287. Consumer Plaintiffs and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to a) damages suffered by Consumer Plaintiffs and Class members as alleged above,

b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

COUNT III

NEGLIGENCE
(ON BEHALF OF CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE NEGLIGENCE CLASSES)

288. Consumer Plaintiffs reallege and incorporate by reference the allegations contained in preceding paragraphs 1-254, as if fully set forth herein.

289. Target owed a duty to Consumer Plaintiffs and members of the statewide Negligence Classes ("Class" as used in this Count III) to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Target's security systems to ensure that Consumer Plaintiffs' and Class members' personal and financial information in Target's possession was adequately secured and protected. Target further owed a duty to Consumer Plaintiffs and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

290. Target owed a duty to Consumer Plaintiffs and members of the Class to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Consumer Plaintiffs and members of the Class who used credit and debit cards to make purchases at Target stores.

291. Target owed a duty of care to Consumer Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate security practices. Target

solicited, gathered, and stored the personal and financial data provided by Consumer Plaintiffs and members of the Class to facilitate sales transactions with its customers. Target knew it inadequately safeguarded such information on its computer systems and that hackers routinely attempted to access this valuable data without authorization. Target knew that a breach of its systems would cause damages to Consumer Plaintiffs and members of the Class and Target had a duty to adequately protect such sensitive financial and personal information.

292. Target owed a duty to timely and accurately disclose to Consumer Plaintiffs and members of the Class that their personal and financial information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Consumer Plaintiffs and members of the Class could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services and take other steps to mitigate or ameliorate the damages caused by Target's misconduct.

293. Consumer Plaintiffs and members of the Class entrusted Target with their personal and financial information, including when using their credit or debit cards to make purchases at Target stores, on the premise and with the understanding that Target would safeguard their information, and Target was in a position to protect against the harm suffered by Consumer Plaintiffs and members of the Class as a result of the Target data breach.

294. Target knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Consumer Plaintiffs and members of the Class who

used credit and debit cards to make purchases at Target stores, and of the critical importance of providing adequate security of that information.

295. Target's own conduct also created a foreseeable risk of harm to Consumer Plaintiffs and members of the Class. Target's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the data breach as set forth herein. Target's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the personal and financial information of Consumer Plaintiffs and Class members.

296. Target breached the duties it owed to Consumer Plaintiffs and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal and financial information of Consumer Plaintiffs and members of the Class.

297. Target breached the duties it owed to Consumer Plaintiffs and Class members by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

298. Target breached the duties it owed to Consumer Plaintiffs and members of the Class by failing to properly maintain their sensitive personal and financial information. Given the risk involved and the amount of data at issue, Target's breach of its duties was entirely unreasonable.

299. Target breached its duties to timely and accurately disclose that Consumer Plaintiffs' and Class members' personal and financial information in Target's possession had been or was reasonably believed to have been, stolen or compromised.

300. Target's failure to comply with its legal obligations and with industry standards and regulations, such as PCI DSS, and the delay between the date of intrusion and the date Target disclosed the data breach further evidence Target's negligence in failing to exercise reasonable care in safeguarding and protecting Consumer Plaintiffs' and Class members' personal and financial information in Target's possession.

301. Target's retention of Consumer Plaintiffs' and Class members' data beyond applicable legal limits, including those imposed by Minn. Stat. § 325E.64, contributed to and facilitated the data breach and further evidences Target's negligence in failing to exercise reasonable care in safeguarding and protecting Consumer Plaintiffs' and Class members' personal and financial data.

302. Target violated Minn. Stat. § 325E.64 by retaining the card security code data, the PIN verification code number, and/or the full contents of Target customers' magnetic stripe data in violation of the statute and the duties it imposes on Target owed to Consumer Plaintiffs and members of the Class.

303. Target knew that Consumer Plaintiffs and members of the Class were foreseeable victims of a data breach of its systems because of laws and statutes that require Target to reasonably safeguard sensitive payment information, including without limitation Minn. Stat. § 325E.64.

304. But for Target's wrongful and negligent breach of its duties owed to Consumer Plaintiffs and members of the Class, their personal and financial information would not have been compromised.

305. The injury and harm suffered by Consumer Plaintiffs and members of the Class as set forth above was the reasonably foreseeable result of Target's failure to exercise reasonable

care in safeguarding and protecting Consumer Plaintiffs' and Class members' personal and financial information within Target's possession. Target knew or should have known that its systems and technologies for processing, securing, safeguarding and deleting Consumer Plaintiffs' and Class members' personal and financial information were inadequate and vulnerable to being breached by hackers.

306. Consumer Plaintiffs and members of the Class suffered injuries and losses described herein as a direct and proximate result of Target's conduct resulting in the data breach, including Target's lack of adequate reasonable and industry-standard security measures. Had Target implemented such adequate and reasonable security measures, Consumer Plaintiffs and Class members would not have suffered the injuries alleged, as the Target data breach would likely have not occurred.

307. A special relationship exists between Consumer Plaintiffs and members of the Class and Target.

308. Target invited Consumer Plaintiffs and members of the Class to use their credit or debit cards in making purchases at Target stores, including during the period of the Target data breach, with the mutual understanding that Target had reasonable security measures in place to protect its customers' personal and financial information.

309. Target's conduct warrants moral blame, as Target continued to take possession of Consumer Plaintiffs' and Class members' personal and financial information in connection with Target sales knowing, and without disclosing, that it had inadequate systems to reasonably protect such information and even after Target received warnings and alerts, including from its own computer systems, that the data breach had occurred and was ongoing, and Target failed to

provide timely and adequate notice to Consumer Plaintiffs and members of the Class as required by law.

310. Holding Target accountable for its negligence will further the policies underlying negligence law and will require Target and encourage similar companies that obtain and retain sensitive consumer personal and financial information to adopt, maintain and properly implement reasonable, adequate and industry-standard security measures to protect such customer information.

311. Target's special relationship with Consumer Plaintiffs and Class members further arises from Target's special and critically important obligations under Minn. Stat. § 325E.64 not to "retain the card security code data, the PIN verification code number, or the full content of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction." Target failed to fulfill its obligations under, and its duties owing to Consumer Plaintiffs and members of the Class arising under, Minn. Stat. § 325E.64 in that Target maintained and continues to maintain the card purchase transaction data covered by the statute beyond the time period it is allowed by law to do so.

312. As a direct and proximate result of Target's negligent conduct, Consumer Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT IV

BREACH OF IMPLIED CONTRACT
(ON BEHALF OF CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE BREACH OF IMPLIED CONTRACT CLASSES)

313. Consumer Plaintiffs incorporate and reallege all allegations contained in

preceding paragraphs 1-254, as if fully set forth herein.

314. When Consumer Plaintiffs and members of the Breach of Implied Contract Classes ("Class" as used in this Count IV) provided their financial and personal information to Target in order to make purchases at Target stores, Consumer Plaintiffs and members of the Class entered into implied contracts with Target pursuant to which Target agreed to safeguard and protect such information and to timely and accurately notify Consumer Plaintiffs and Class members that their data had been breached and compromised.

315. Target solicited and invited Consumer Plaintiffs and members of the Class to purchase products at Target stores using their credit or debit cards. Consumer Plaintiffs and members of the Class accepted Target's offers and used their credit or debit cards to purchase products at Target stores during the period of the Target data breach.

316. Each purchase made at a Target store by Consumer Plaintiffs and members of the Class using their credit or debit card was made pursuant to the mutually agreed upon implied contract with Target under which Target agreed to safeguard and protect Consumer Plaintiffs' and Class members' personal and financial information, including all information contained in the magnetic stripe of Consumer Plaintiffs' and Class members' credit or debit cards, and to timely and accurately notify them that such information was compromised and breached.

317. Consumer Plaintiffs and Class members would not have provided and entrusted their financial and personal information, including all information contained in the magnetic stripes of their credit and debit cards, to Target in order to purchase products at Target stores in the absence of the implied contract between them and Target.

318. Consumer Plaintiffs and members of the Class fully performed their obligations under the implied contracts with Target.

319. Target breached the implied contracts it made with Consumer Plaintiffs and Class members by failing to safeguard and protect the personal and financial information of Consumer Plaintiffs and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of Target data breach.

320. The losses and damages sustained by Consumer Plaintiffs and Class members as described herein were the direct and proximate result of Target's breaches of the implied contracts between Target and Consumer Plaintiffs and members of the Class.

COUNT V

BREACH OF REDCARD AGREEMENTS
(ON BEHALF OF REDCARD DEBIT CARD HOLDER CONSUMER PLAINTIFFS AND THE NATIONWIDE REDCARD CLASS)

321. Consumer Plaintiffs incorporate and reallege the allegations contained in preceding paragraphs 1-254, as if fully set forth herein.

322. Target offers a branded debit card called the Target Debit Card. Target also offers Target branded credit cards, including the Target Credit Card. Target previously offered a Target Visa credit card. Collectively, these cards are referred to here as "Target REDcards" or "REDcard(s)."

323. Consumer Plaintiffs and members of the nationwide REDcard Debit Card Class who have a Target REDcard debit card ("Class" as used in this Count V), are subject to an agreement with Target called the Target Debit Card Agreement. Target incorporates its Target Debit Card Privacy Policy into the terms of the Target Debit Card Agreement. As a condition of receiving their Target REDcard debit cards, Consumer Plaintiffs and REDcard Class members who have a Target REDcard debit card are subject to the terms of the Target Debit Card Agreement and the Target Debit Card Privacy Policy incorporated into that Agreement.

324. The Target Debit Card Agreement provides: "You agree to our collection, use and sharing of information about your EFT as provided in Target Debit Card Privacy Policy ('Privacy Policy'), which is included as part of this Agreement."

325. The Target Debit Card Privacy Policy states: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."

326. The Target Debit Card Agreement provides: "17. **WHAT LAW APPLIES –** This agreement will be governed by federal law and to the extent state law applies, by the law of South Dakota. If there is any conflict between any of the terms and conditions of this Agreement and applicable federal or state law, this Agreement will be considered changed to the extent necessary to comply with the law."

327. Each purchase made at a Target store by Consumer Plaintiffs and by members of the Class using their Target REDcard debit card was made subject to the uniform, common terms of the Target Debt Card Agreement and the Target Debit Card Privacy Policy.

328. Consumer Plaintiffs and members of the REDcard Class fully performed their obligations under the above agreements and documents.

329. Target breached the Target Debit Card Agreement and the Target Debit Card Privacy Policy. Contrary to the terms of the agreements, and by engaging in the conduct set forth in this Complaint, Target did not protect its customers' personal information from unauthorized access and use and Target did not use measures, including computer safeguards and secured files and buildings, to protect Consumer Plaintiffs' and Class members' personal information from unauthorized access and use.

330. Consumer Plaintiffs and members of the REDcard Class used their Target REDcard debit cards to make purchases at Target stores during the period of the Target data breach. Their Target REDcard debit cards were compromised in and as a result of the Target data breach. Consumer Plaintiffs and members of the REDcard Class suffered damages and losses as described herein.

331. The damages and losses sustained by REDcard debit card holder Consumer Plaintiffs and members of the REDcard Class are the direct and proximate result of Target's breaches of the Target Debit Card Agreement and the Target Debit Card Privacy Policy.

COUNT VI

BAILMENT
(ON BEHALF OF CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE BAILMENT CLASSES)

332. Consumer Plaintiffs incorporate and reallege the allegations contained in preceding paragraphs 1-254, as if fully set forth herein.

333. Consumer Plaintiffs and members of the separate statewide Bailment Classes ("Class" as used in this Count VI) delivered their personal and financial information, including the information contained on the magnetic stripes of their credit or debit cards, to Target for the exclusive purpose of making purchases from Target at Target stores.

334. In delivering their personal and financial information to Target, Consumer Plaintiffs and Class members intended and understood that Target would adequately safeguard their personal and financial information.

335. Target accepted possession of Consumer Plaintiffs' and Class members' personal and financial information for the purpose of accepting payment for goods purchased by Consumer Plaintiffs and members of the Class at Target stores.

336. By accepting possession of Consumer Plaintiffs' and Class members' personal and financial information, Target understood that Consumer Plaintiffs and Class members expected Target to adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

337. During the bailment (or deposit), Target owed a duty to Consumer Plaintiffs and Class members to exercise reasonable care, diligence and prudence in protecting their personal and financial information.

338. Target breached its duty of care by failing to take appropriate measures to safeguard and protect Consumer Plaintiffs' and Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Consumer Plaintiffs' and Class members' personal and financial information.

339. Target further breached its duty to safeguard Consumer Plaintiffs' and Class members' personal and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the Target data breach.

340. Target failed to return, purge or delete the personal and financial information of Consumer Plaintiffs and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

341. As a direct and proximate result of Target's breach of its duty, Consumer Plaintiffs and Class members suffered consequential damages that were reasonably foreseeable to Target, including but not limited to the damages set forth above.

342. As a direct and proximate result of Target's breach of its duty, the personal and financial information of Consumer Plaintiffs and Class members entrusted to Target during the bailment (or deposit) was damaged and its value diminished.

COUNT VII

UNJUST ENRICHMENT
(ON BEHALF OF CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE UNJUST ENRICHMENT CLASSES)

343. Consumer Plaintiffs fully incorporate by reference the allegations contained in preceding paragraphs 1-254, as if fully set forth herein.

344. Consumer Plaintiffs and members of the separate statewide Bailment Classes ("Class" as used in this Count VII) conferred a monetary benefit on Target in the form of monies paid for the purchase of goods from Target during the period of the Target data breach.

345. Target appreciates or has knowledge of the benefits conferred directly upon it by Consumer Plaintiffs and members of the Class.

346. The monies paid for the purchase of goods by Consumer Plaintiffs and members of the Class to Target during the period of the Target data breach were supposed to be used by Target, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Consumer Plaintiffs and members of the Class.

347. Target failed to provide reasonable security, safeguards and protection to the personal and financial information of Consumer Plaintiffs and Class members and as a result, Consumer Plaintiffs and Class members overpaid Target for the goods purchased through use of their credit and debit cards during the period of the Target data breach.

348. Under principles of equity and good conscience, Target should not be permitted to retain the money belonging to Consumer Plaintiffs and members of the Class, because Target failed to provide adequate safeguards and security measures to protect Consumer Plaintiffs' and Class members' personal and financial information that they paid for but did not receive.

349. As a result of Target's conduct as set forth in this Complaint, Consumer Plaintiffs and members of the Class suffered damages and losses as stated above, including monies paid

for Target products that Consumer Plaintiffs and Class members would not have purchased had Target disclosed the materials facts that it lacked adequate measures to safeguard customers' data and had Target provided timely and accurate notice of the data breach, and including the difference between the price they paid for Target's goods as promised and the actual diminished value of its goods and services.

350. Consumer Plaintiffs and the Class have conferred directly upon Target an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Consumer Plaintiffs and the Class.

351. The economic benefit, including the monies paid and the overcharges and profits derived by Target and paid by Consumer Plaintiffs and members of the Class, is a direct and proximate result of Target's unlawful practices as set forth in this Complaint.

352. The financial benefits derived by Target rightfully belong to Consumer Plaintiffs and members of the Class.

353. It would be inequitable under established unjust enrichment principles in the District of Columbia and all of the 50 states for Target to be permitted to retain any of the financial benefits, monies, profits and overcharges derived from Target's unlawful conduct as set forth in this Complaint.

354. Target should be compelled to disgorge into a common fund for the benefit of Consumer Plaintiffs and the Class all unlawful or inequitable proceeds received by Target.

355. A constructive trust should be imposed upon all unlawful or inequitable sums received by Target traceable to Consumer Plaintiffs and the Class.

356. Consumer Plaintiffs and the Class have no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Consumer Plaintiffs, on behalf of themselves and the Classes set forth herein, respectfully request the following relief:

A. That the Court certify this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2) and (b)(3), and, pursuant to Fed. R. Civ. P. 23(g), appoint the named Consumer Plaintiffs to be Class representatives and their undersigned counsel to be Class counsel;

B. That the Court award Consumer Plaintiffs and the Classes appropriate relief, including actual and statutory damages, restitution and disgorgement;

C. That the Court award Consumer Plaintiffs and the Class equitable, injunctive and declaratory relief as maybe appropriate under applicable state laws. Consumer Plaintiffs, on behalf of the Classes, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information and that would include, without limitation, an order and judgment directing Target to 1) encrypt all sensitive cardholder data beginning within the device to which the cards are presented for purchase (e.g., PINpad) and continuing until the data reaches Target's payment processor or payment switch; 2) comply with the Payment Card Data Security Standard (PCI DDS); 3) comply with Minn. Stat. § 325E.64 , by ceasing to retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction, and comply with similar applicable laws and standards; 4) with respect to Target REDcards or any other Target credit or debit card issued by or on behalf of Target,

Target shall adopt and use EMV chip technology; and 5) directing Target to provide to Consumer Plaintiffs and Class members extended credit monitoring services.

D. That the Court award Consumer Plaintiffs and the Classes pre-judgment and post-judgment interest;

F. That the Court award Consumer Plaintiffs and the Classes reasonable attorney fees and costs as allowable by law;

G. Such additional orders or judgments as maybe necessary to prevent these practices and to restore any interest or any money or property which may have been acquired by means of the violations set forth in this Complaint;

H. That the Court award Consumer Plaintiffs and the Classes such other, favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Consumer Plaintiffs demand a trial by jury on all issues so triable.

Date: December 1, 2014

s/ *Vincent J. Esades*

Vincent J. Esades (249361)
David Woodward (018844X)
HEINS MILLS & OLSON, P.L.C.
310 Clifton Avenue
Minneapolis, MN 55403
Tel.: (612) 338-4605
Fax: (612) 338-4692
vesades@heinsmills.com
dwoodward@heinsmills.com

Lead Counsel Consumer Cases

E. Michelle Drake (0387366)
NICHOLS KASTER, PLLP
4600 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Tel.: (612) 256-3200

Fax: (612) 338-4878
drake@nka.com

Liaison Counsel Consumer Cases

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP, PA
201 North Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
Fax: (813)-223-5402
jyanchunis@forthepeople.com

Executive Committee - Coordinating Lead and Liaison Counsel

Daniel C. Girard
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, CA 94108
Tel.: (415) 981-4800
Fax: (415) 981-4846
DCG@girardgibbs.com

Ariana J. Tadler
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, NY 10119
Tel.: (212) 594-5300
Fax: (212) 868-1229
atadler@milberg.com

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel.: (816) 714-7100
Fax: (816) 714-7101
siegel@stuevesiegel.com

Steering Committee Consumer Cases